

Nemzeti Közsolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar
Katonai Üzemeltető Intézet
Informatikai és Elektronikai Hadviselés Tanszék
Informatikai Szakcsoport

**A vékony kliens számítógép-architektúra Magyar Honvédségben
történő alkalmazhatóságának vizsgálata**

Tudományos Diákköri dolgozat

A témavezető neve, beosztása

Szabó András főhadnagy, tanársegéd

Készítette:

Dávid Balázs honvédtiszt-jelölt

Budapest

2014.

Tartalomjegyzék

Bevezetés	2
1. A katonai célú számítógépes rendszerek felhasználási területei, a jelenlegi rendszer hiányosságai.....	4
1.1 A stacioner kommunikációs rendszer jellemzői	4
1.2 A tábori hírendszer	5
1.3 A katonai számítógépes rendszer hiányosságai	6
2. Legacy PC-k felügyeletének és üzemeltetésének lehetőségei	8
2.1. A rendszergazda feladatai	8
2.2 Legacy eszközök a rendszerben	11
3. A vékony kliens architektúra bemutatása	14
3.1 Történeti áttekintés	14
3.2 A vékony kliens architektúra alapjai.....	16
3.3 A vékony kliensek működése	17
3.4 A vékony kliensekkel elérhető szolgáltatások	17
3.5 Az adatközpontok	18
3.6 A kapcsolattartáshoz használt protokollok	18
3.7 A hálózattal szemben támasztott követelmények	19
4. A vékony kliens architektúra előnyei és hátrányai	20
4.1. Előnyei az asztali számítógépekkel szemben.....	20
4.2. Lehetséges hátrányai	22
5. A különböző zárt és nyílt forráskódú operációs rendszerekkel ellátott kliensek katonai célú alkalmazhatóságának vizsgálata	25
5.1 Vékony kliens eszközök.....	25
5.2 Meglévő asztali számítógépek újra felhasználásának lehetőségei.....	27
5.3 A meglévő hálózat vizsgálata a vékony kliens architektúra szükségleteinek szempontjából.....	29
5.4 Élet a Microsofton túl	31
5.5 Vékony kliens jellegű eszközök tábori alkalmazhatósága	34
Befejezés	39
Irodalomjegyzék	41
Ábrajegyzék	43

BEVEZETÉS

Az elmúlt évtizedek robbanásszerű számítástechnikai fejlődése, az eszközök drasztikus sebességnövekedése és az ebből eredő jelentős mértékű számítógép központúság mindennapi életünk részévé vált. A számítógépek és a számítógépes hálózatok mindenhol velünk vannak, a kenyérpirítótól elkezdve, a mobiltelefonunkon át egészen a repülésirányításig. A korábbi speciális eszközöket igénylő feladatokat ma már egységes, számítógép vezérelt platformok látják el. Ezen technológiák nem maradtak meg a civil szféra berkeiben. A korszerű hadseregek számára fontossá vált a modern technológiák alkalmazása, ezzel elősegítve a tervezés és a döntéshozás folyamatát, valamint az együttműködést más, szövetséges országok katonai szervezeteivel, a minél magasabb szintű interoperabilitás megteremtése érdekében. Az új szolgáltatásokat, technológiákat azonban csak akkor lehet kihasználni, ha az azokat kiszolgáló informatikai rendszerek is korszerűek.

A hadszínterek ma már nem korlátozódnak csupán a harcmezőkre, egy újfajta fenyegetéssel is szembe kell néznünk. A kiber, vagy információs hadviselés legalább annyira veszélyes, mint a konvencionális fegyverek alkalmazása. A számítógépes infrastruktúrák támadása ma már mindennapi probléma a nemzetállamok számára. Ezeknek a hálózatok a támadásával és a sérülékenységek kihasználásával komoly anyagi károkat lehet okozni a megtámadott országnak. De nem feledkezhetünk meg arról sem, hogy Magyarország egy katonai szövetség, a NATO tagja. Ez informatikai jellegű kötelezettségeket és feladatokat is ró az országra, a Magyar Honvédségre. Szövetségeseknek is igen nagy problémát jelentene, ha a NATO hálózatába illetéktelen úgy jutnának be, hogy valamilyen magyarországi rendszer hálózati gyengeségét használnák ki. Különös tekintettel az ország szövetségi helyzetére, úgy gondolom, hogy a Honvédség folytonos fenyegetettségnek van kitéve, így bármikor támadások érhetik a számítógépes rendszereit. A hálózati és informatikai biztonság a legfőbb szereplői az információk és adatok védelmének, és megőrzésének. Éppen ezért fontos egy olyan központosított és egységes számítógépes rendszer kialakítása, mely megfelel a műveleti és doktrínális szabályozásoknak is. A Honvédség számára olyan számítógépes rendszert és hálózatot kell létrehozni, mely lehetővé teszi minden végfelhasználói számítógép egységes felügyeletét. Jelenleg a sérülékenységek nagy részéért a kliens oldali sebezhetőségek a felelősek. Ha ezekre a végfelhasználói pontokra is kiterjeszthetők lennének a

központosított hibajavítási metódusok és frissítések, akkor számottevő mértékben csökkenne a hálózat sebezhetősége.

Fontosnak tartom, hogy foglalkozzunk a fent említett új hadviselési formával, azokkal a technikai megoldásokkal melyek lehetővé teszik, hogy a fenyegetettség mértékét minimális szintre lehessen csökkenteni. Témaválasztásom ezért esett a vékony kliens architektúrára. Dolgozatomban áttekintem a jelenlegi rendszer összetevőit, a kommunikációs hálózatokat, különös tekintettel azok informatikai vonatkozásaira valamint a meglévő számítógépes rendszer hiányosságaira. Ezután bemutatásra kerül a vékony kliens architektúra kialakulása, fejlődése, valamint rávilágítok a technológia előnyeire és hátrányaira is. Végül bemutatásra kerülnek azok a jelenleg is piacon lévő eszközök és megoldások, melyekkel megvalósítható lenne a vékony kliensek bevezetése a Magyar Honvédségbe.

1. A KATONAI CÉLÚ SZÁMÍTÓGÉPES RENDSZEREK FELHASZNÁLÁSI TERÜLETEI, A JELENLEGI RENDSZER HIÁNYOSSÁGAI

Egy szervezet vezetéséhez elengedhetetlen a szükséges információk rendelkezésre állása. A szervezet rendeltetésszerű működéséhez szükséges információfeldolgozást ma már számítógépes rendszerek segítik. Ezek a rendszerek olyan szolgáltatásokat nyújtanak, melyek ma már a katonai vezetés és irányítás hatékonyságának alapvető feltételei. De nem csak a vezetés hatékonyságát növeli, hanem a mindennapi, békeidőben fellépő feladatok megoldását is elősegíti. Ezeknek a feladatoknak az elvégzése napjainkban elképzelhetetlen egy állandó telepítésű kommunikációs hálózat nélkül. Az előjáró szervek és az alárendelt alakulatok közötti kapcsolattartás az ilyen fix telepítésű hálózatokon keresztül valósul meg. Azonban maga a kommunikációs hálózat önmagában értéktelen, ha nincsenek hozzákapcsolva a végpontok, azaz a felhasználók. A mai rohamléptekben fejlődő számítástechnika tükrében fontos megvizsgálni a meglévő rendszereket az új technológiai vívmányok alkalmazhatóságának szempontjából is.

A Magyar Honvédségben a végfelhasználók számára az elérhető számítástechnikai eszközöket a személyi számítógépek jelentik. A felhasználók egy olyan, inhomogén számítógépes környezetben dolgoznak, mely megnehezíti a hálózat és a rendszer védelmét, támogatását, felügyeletét valamint az eszközök és alkalmazások kezelhetőségét. Ezek összessége végül inkább negatív irányba befolyásolja a felhasználói tapasztalatot, mely végső esetben hanyag munkavégzéshez is vezethet. Véleményem szerint ezzel a problémával foglalkozni kell, és ahogyan a fejezet későbbi részében olvasható, nem a gyenge felhasználói élmény miatt.

1.1 A stacioner kommunikációs rendszer jellemzői

Az állandó telepítésű kommunikációs és informatikai hálózat¹ biztosítja az országban szétszórtnan elhelyezkedő alakulatok számára azt a lehetőséget, hogy ezen keresztül csatlakozzanak a honvédség belső (Intranet) hálózatához, az Internethez, valamint ezen keresztül lehet kapcsolatot létesíteni a NATO információs rendszerével is. A Honvédségben biztosított informatikai szolgáltatásokat is ezen keresztül éri el az alakulatok.

Az állandó telepítésű hálózatban jelenleg két digitális átviteli megoldást alkalmaznak, az egyik az időosztásos átvitel (TDM), a másik az IP alapú adatátvitel. Ennek

¹ MH Kormányzati Célú Elkülönült Hírközlő Hálózat, 346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról, 2. melléklet

a kettősségnek az oka az, hogy a korábban meglévő távközlő hálózatra épült rá az informatikai szolgáltatásokat is kiszolgáló hálózat. Mára azonban a hálózati forgalom nagymértékben eltolódott az adathálózati alapú forgalom irányába. Ennek megfelelően az adatátvitel fejlesztése is az IP alapú eszközök és módszerek fejlesztésével és alkalmazásával valósulhat meg.

A hálózat nagymértékben inhomogén, átviteli közegek tekintetében mind vezetékes, mind vezeték nélküli megoldásokat is találhatunk. Ez a különbözőség a jelenleg elérhető sávszélességeken is nyomon követhető, hiszen az adatátviteli sebesség 10Gbit/sec-től 2Mbit/sec-ig terjed. Az átviteli sebesség alsó határa csak a meglévő szolgáltatások eléréséhez elegendő, ha még több központi szolgáltatás kerül bevezetésre, melyek kiszolgáló központja Budapesten található, akkor elkerülhetetlenné válik a kommunikációs hálózat kapacitásának jelentős mértékű növelése. Ez azonban szükségszerűen magával vonja a jelenlegi hálózati forgalom mélyebb vizsgálatát és esetlegesen a hálózati, és kiszolgáló eszközök fejlesztését is.

1.2 A tábori hírendszer

A tábori, műveleti körülmények között is alkalmazható hírhálózati rendszerek megléte és alkalmazása szinte már létfontosságú egy korszerű hadsereg számára. Ezen eszközök célja a vezetési és irányítási feladatok biztosítása. Ennek megfelelően a Magyar Honvédség is rendelkezik tábori informatikai képességgel. Az alkalmazott rendszer a NATO igényeinek is eleget tevő tábori vezetési és irányítási rendszerből és a hozzá kapcsolódó tábori híradó és informatikai központból áll. A központon keresztül lehetőség van műholdas kapcsolaton keresztül kapcsolódni a Magyar Honvédség állandó telepítésű hálózatára, és az ott lévő szolgáltatásokat igénybe venni.

A hazai gyakorlat azt mutatja, hogy a kitelepülések során, a felhasználók a magukkal vitt (értsd: az irodai) személyi számítógépeket használják. Jelentős problémákat vetnek fel a használatban lévő számítástechnikai eszközök. Egyfelől ezek a személyi számítógépek hordozhatósága hagy némi kívánni valót maguk után- (attól függetlenül, hogy laptopokról, vagy asztali személyi számítógépekről van szó. Másrészt ezek az eszközök nem a csúcstechnikát jelentik, jellemzően egy kiöregedő géppark részei, egy gyártói támogatás nélküli operációs rendszerrel. Ha egy ilyen eszközökből kialakított hálózatot felcsatlakoztatjuk a stacioner hálózatra, akkor az jelentős kockázatot jelent a hálózatra. Elsősorban biztonsági szempontból kockázatos, ugyanis ezeken a

számítógépeken megbújhatnak olyan kártevők, amelyek csak alkalomra várnak, hogy megfertőzhessék az egész hálózatot.

1.3 A katonai számítógépes rendszer hiányosságai

A Magyar Honvédség jelenlegi informatikai jellegű igényeit a meglévő hálózat ki tudja szolgálni. Azonban mind a szolgáltatásokat kiszolgáló eszközpark, mind pedig a hálózati infrastruktúra másik, felhasználói oldalán lévő számítógépek kiöregedő félben vannak. A katonai szervezeteknél legnagyobb arányban elterjedt Windows XP operációs rendszerhez vásárolt asztali számítógépek legalább olyan időssek, mint a rajtuk futó operációs rendszer, melynek legelső változatát 2001. október 25-én adták ki. A számítástechnikában ez a több mint tíz év nagyon hosszú időnek számít. Például csak a Microsoft három másik, kliens operációs rendszert fejlesztett ki azóta, a szervizcsomagokat nem számolva. A kiszolgálóknál sem jobb a helyzet, ott is találkozhatunk még az XP után nem sokkal megjelent Microsoft Windows Server 2003 operációs rendszert futtató szerverrel.

A kiöregedő számítástechnikai eszközök és a rajtuk futó szoftverek jelenlegi rendszerben tartása önmagában nem feltétlenül jelent problémát. Hiszen a mindennapok során azt tapasztaljuk, hogy ezek a rendszerek működnek, kiszolgálják a felhasználói igényeket. A problémát az jelenti, hogy az említett asztali operációs rendszernek 2014. április 8-án lezárult a bővített támogatási időszaka. Ez azt jelenti, hogy a továbbiakban felmerülő problémákat, az újonnan felfedezett biztonsági réseket a gyártó már nem fogja javítani. Ha ez nem lenne elég nagy probléma, 2015. júliusában a szerver verzió támogatása is megszüntetésre kerül. A támogatás megszűnése magával hozza majd a harmadik fél által gyártott szoftverek és eszközillesztő-programok támogatásának megszűnését is. Hiszen gondoljunk csak bele, egy fejlesztőcégnek sem éri majd meg olyan operációs rendszerre fejleszteni a saját programját, amelyet már az azt kiadó vállalat sem támogat. Előbb vagy utóbb – véleményem szerint inkább utóbb, ahogy a vállalati döntéshozók és az otthoni felhasználók viszonyulnak most az XP leváltásához – egyszerűen már nem lehet majd olyan alkalmazásokat vásárolni, melyek ezen a régi operációs rendszeren is elindulnak. Sőt, ez a probléma visszafelé is fennáll. Hiába vásárolunk egy új eszközt, ha azt a régi operációs rendszer nem ismeri fel, vagy nem tud azzal kommunikálni. Elég sok álmatlan éjszakát okozhat a rendszermérnöknek egy-egy új eszköz integrálása a már meglévő számítógépes környezetbe.

1.3.1 A rendszer sebezhetősége

Ahogy az már az előző bekezdésben is említettem, a terméktámogatás megszűnése azért jelent különösen nagy kockázatot, mert a feltárolt hibák nem kerülnek javításra. Minden újonnan felfedezett sebezhetőség attól a pillanattól kezdve, hogy napvilágra került, nulladik napi sebezhetőség marad. Javítócsomagok nélkül nem záródik be a sebezhetőségi ablak. A hosszú ideig nem javított hibák nem csak a profi támadóknak teremtenek lehetőséget a behatolásra, hanem a script kiddie-k² számára is. Egy ilyen nagymértékben elterjedt operációs rendszer esetében azzal kell számolnunk, hogy a támadók is nagy figyelmet fordítanak rá, különös tekintettel akkor, mikor biztosra vehető, hogy az újonnan felfedezett hibák nem kerülnek javításra.

Azonban nem csak magának az operációs rendszernek a sérülékenysége jelenthet problémát. Még ha az XP teljesen biztonságos is lenne, az alkalmazások szintjén akkor is előfordulhatnak sebezhetőségek. Mint már említettem, egy nem támogatott operációs rendszerre nagy valószínűséggel a szoftverfejlesztés is le fog állni. Itt most nem csak arra kell gondolni, hogy új programok nem fognak megjelenni a régi rendszerre, hanem arra is, hogy az alkalmazások frissítései is elmaradoznak majd. Ha figyelembe vesszük a Java, vagy a Flash sebezhetőségét, ez jelentős biztonsági kockázatot jelent. Egy Kaspersky Lab által készített jelentés szerint, mely 2012. szeptembere és 2013. augusztusa között gyűjtött adatokra alapoz, több mint 160 Java-hoz kapcsolódó sebezhetőség került napvilágra, ezek közül hat volt kritikus, valamint több mint 14,1 millió támadást regisztráltak, melyek valamilyen Java sebezhetőséget használtak ki. Ne feledjük, hogy ezek a támadások egy támogatási ciklusban lévő alkalmazás sebezhetőségét használták ki. A támogatás megszűnése azonban nem fogja megszüntetni a támadásokat is.

² Azon, jellemzően fiatal személyek, akik nem létező, vagy csekély informatikai, programozói tudással, az Interneten talált kódokat felhasználva használnak ki biztonsági sebezhetőségeket.

2. LEGACY PC-K FELÜGYELETÉNEK ÉS ÜZEMELTETÉSÉNEK LEHETŐSÉGEI

A számítógép mindennapi életünk részévé vált. Ma már számítógépek, számítógépes rendszerek nélkül egyetlen szervezet sem létezhet, a mindennapos munkavégzés szerves velejárója. Mindaddig nem is igazán veszünk tudomást ezekről a rendszerekről, amíg hiba nélkül működnek. Azonban elég pár perc szolgáltatás kimaradás és jobb esetben csak néhány felhasználói e-mail nem érkezik meg időben, rosszabb esetben akár emberéletek is veszélybe kerülhetnek. Ezért fontos feladat tehát ezeknek a számítógépes rendszereknek a felügyelete, üzemeltetése.

A rendszer felügyelet az a munkaterület, melynek során az ezzel megbízott személy vagy személyek egy, vagy több rendszer szoftveres, hardveres összetevőit üzemeltetik. Célja a rendszer hatékony és eredményes működésének biztosítása.

A rendszergazdák feladatai közé tartoznak a különböző biztonsági beállítások megfigyelése, ellenőrzése, a felhasználói fiókok kezelése, karbantartása, a különböző erőforrások megfigyelése, biztonsági mentések végrehajtása valamint új hardver és szoftvereszközök telepítése és beállítása.

2.1. A rendszergazda feladatai

A következő részben áttekintésre és összegzésre kerülnek azok az alapvető feladatok, amelyeket egy rendszergazdának várhatóan végre kell hajtani a rendszer üzemeltetése során. Ezek a feladatok nem feltétlenül korlátozódnak egy személyre, általában több ember között oszlanak meg. Éppen ezért fontos, hogy legyen legalább egy valaki, aki a rendszer minden összetevőjét megérti, átlátja azok működését, és meg tud róla győződni, hogy saját feladatát mindenki megfelelően látta el.

2.1.1 Hardvereszközök hozzáadása és eltávolítása

Egy új hardver beszerelése vagy egy hardver másik gépbe történő átszerelése után a rendszert be kell állítani, hogy felismerje az új hardverösszetevőt és megfelelően használja azt. A hardverek kezelése széles skálán mozoghat az egyszerű feladatoktól, mint egy nyomtató rendszerbe állítása, a sokkal összetettebb feladatokig, mint például egy lemez tömb³ beszerelése.

Napjainkban a virtualizáció nagymértékű elterjedése sem egyszerűsítette ezeket a feladatokat. Az eszközök telepítését a virtualizációs réteg több szintjén is el kell végezni,

³A lemez tömb egy olyan hardver összetevő, mely több merevlemezt tartalmaz.

és különböző irányelvek kialakítására és alkalmazására is szükség lehet a megfelelő biztonság elérése érdekében.

2.1.2 Szoftverek telepítése és frissítése

Egy-egy új szoftver beszerzését követően célszerű azt telepíteni és tesztelni vegyes hardver és szoftver környezetben. Mikor meggyőződünk róla, hogy a szoftver megfelelően működik, telepítésre kerülhet a felhasználói számítógépekre is. Így az esetleges nem rendeltetésszerű működésből eredő problémák kijavíthatóak, és a felhasználók már csak a jól működő, kevésbé hibás szoftverrel találkoznak. A szoftverhez kiadott javítócsomagok és frissítések felhasználói környezetben történő zökkenőmentes alkalmazása is a rendszergazdai feladatok körébe tartozik.

2.1.3 A rendszer ellenőrzése

Minél nagyobb egy számítógépes rendszer, minél több gépből áll, annál nagyobb odafigyelést igényel. A felhasználók jellemzően csak a komoly hibákat jelzik, a kisebbeket nem. Előfordulhat, hogy egy probléma megkerülése gyorsabb, mint jelteni azt a megfelelő személy számára, így a felhasználók a kisebb ellenállás irányába indulhatnak el.

Rendszeresen ellenőrizzük a futó szolgáltatások megfelelő működését, egy-egy hiba korai előjeleit mutathatják a naplófájlok is, így azok gyakori kontrollja segíthet a helyes működés fenntartásában. Fontos szemmel tartani a rendelkezésre álló erőforrásokat is, mint például a lemezterületet. Ezeket az ellenőrzési feladatokat természetesen automatizálhatjuk is, és számos program segítheti a rendszergazda ellenőrzési feladatait.

2.1.4 Felhasználói fiókok felügyelete

A rendszeradminisztrátori feladatokhoz kapcsolódik a felhasználói fiókok kezelése. Ebbe bele tartozik az új fiókok létrehozása, a már nem aktív felhasználókhoz tartozó fiókok törlése, valamint minden olyan feladat, ami a felhasználói fiókokhoz köthető.

Ha egy felhasználó rendszerhez történő hozzáférése megszüntetésre kerül, akkor a felhasználói fiókját le kell tiltani. A fiókjához tartozó fájlokat egy biztonsági mentés során el kell menteni, majd azokat az eredeti helyükről törölni kell, így a már nem használt fájlok és felhasználói adatok felgyülemzése elkerülhető.

2.1.5 Biztonsági mentések készítése

A biztonsági mentések készítése a legfontosabb rendszergazdai feladatok közé tartozik. Lehet, hogy unalmas és időigényes munka, de mindenképpen szükséges. A

biztonsági mentés folyamatát is lehet ugyan automatizálni, de ettől függetlenül a rendszergazda feladata ellenőrizni, hogy a biztonsági mentés megfelelően, a tervezett időben került végrehajtásra. Fontos megjegyezni, hogy nem elég a biztonsági mentés meglétét ellenőrizni, arról is meg kell bizonyosodni, hogy az elmentett adatok a megfelelő módon vissza is állíthatóak.

2.1.6 Biztonsági ellenőrzések

A rendszerhez kapcsolódó biztonsági rendelkezések betartásának ellenőrzése szintén a rendszergazda feladata. Ez széles skálán mozoghat a jogosulatlan hozzáférések ellenőrzéstől, a komplikált hálózati behatolást detektáló programok felügyeletéig.

2.1.7 Hibaelhárítás

Elkerülhetetlen, hogy egy rendszer bizonyos részei meghibásodjanak. Az rendszergazda feladata ezeknek a hibáknak a felderítése és kijavítása. Megtalálni egy-egy problémát gyakran nehezebb, mint kijavítani azt.

2.1.8 A helyi rendszerhez tartozó dokumentáció elkészítése

Ahogy az előzetes tervek alapján kiépített rendszeren változások történnek, úgy kell ezeket a változásokat a rendszergazdának a rendszerhez tartozó dokumentációba bevezetnie. Az ő feladata tehát nem csak a változások életbe léptetése, az új hardverek beszerelése, de ezeknek a változásoknak a megfelelő dokumentálása is, a könnyebb nyomon követhetőség érdekében. Ez a feladat magában foglal minden, a rendszer fizikai felépítéséhez kapcsolódó leírást, a hardverek karbantartási jegyzőkönyveit valamint a különböző biztonsági mentések állapotait is. Sőt, nem elég a biztonsági eljárásokat és szabályzatokat bevezetni, azok meglétét, betartását és betartatását megfelelően dokumentálni is kell.

2.1.9 Felhasználói segítségnyújtás

A rendszerfelügyelet azonban nem csak hardverek és szoftverek telepítéséről szól. Az egész lényege egy olyan számítógépes rendszer tervezése és megépítése, amely azt a célt szolgálja, hogy a felhasználók elvégezhessék a munkájukat.

Habár nem feltétlenül tartalmazza a rendszergazdák munkaköri leírása a felhasználók problémáinak megoldását, ez mégis jelentős plusz munkát jelent. Ezek főként felhasználói figyelmetlenségből eredő problémák, de mégis jelentős időt vonhat el a tényleges felügyeleti munkától.

2.2 Legacy eszközök a rendszerben

A számítástechnikában az ún. legacy rendszerek a régi, elavult technológiákat, számítógépes rendszereket jelölik. Értelem szerűen beszélhetünk elavult rendszerekről mind szoftveres, mind hardveres tekintetben. Annak, hogy ezek az eszközök miért maradnak használatban, számos oka lehet. Vannak olyan esetek, amikor ezekre a régi rendszerekre készített megoldások tudják csak kiszolgálni egyes ügyfelek speciális igényeit. Vagy amikor az alkalmazási környezet nem változott az évek során, a régi rendszerek ugyanúgy használhatóak maradnak.



1. ábra: IBM személyi számítógép

Az elavult technológiák használatban tartásának azonban van néhány lehetséges mellékhatása, sőt veszélye is.

- A legacy rendszerek jellemzően elavult és lassú hardvereken futnak, melyek javíttatása, cseréje az idő előrehaladtával egyre nehezebb és egyre drágább lesz.
- Egy elavult rendszer fenntartása magasabb költséget róhat a fenntartó szervezet számára, mintha azt teljes egészében (mind a hardvert, mind a szoftvert) lecserélnék.
- Ezeket a rendszereket nehéz bővíteni, újítani, mert az új hardverek és szoftverek inkompatibilitási problémákat jelenthetnek. A régi szoftver nem fut az új hardveren, az új szoftver nem fut a régi hardveren.
- Azonban ezeknek a régi rendszereknek a legnagyobb hátránya a sebezhetőségük. Az olyan operációs rendszerek és alkalmazások további használata, melyeknek megszűnt a támogatása, és így már nem jelennek meg hozzájuk biztonsági frissítések, jelentős veszélyt jelentenek az egész szervezet számára. Ezek a szoftverek válnak a támadók elsődleges célpontjaivá, hiszen a felfedezésre kerülő biztonsági hibákat már senki nem fogja kijavítani.

2.2.1 A biztonsági kockázatok csökkentésének lehetőségei

Az elektronikus információs rendszerek olyan fenyegetéseknek vannak kitéve, melyek sérthetik azok védettségét, biztonságát. A kockázat pedig valamilyen fenyegető tényezőtől eredő fenyegetettség mértéke. A rendszer biztonsági kockázata több tényezőtől

épül fel, ennek egyik eleme, egy adott fenyegetés bekövetkezésének valószínűsége. Ahhoz, hogy ezt csökkenteni tudjuk, számos, elsősorban szoftveres megoldás áll rendelkezésre.

Ilyen például a Microsoft EMET eszközkészlet.

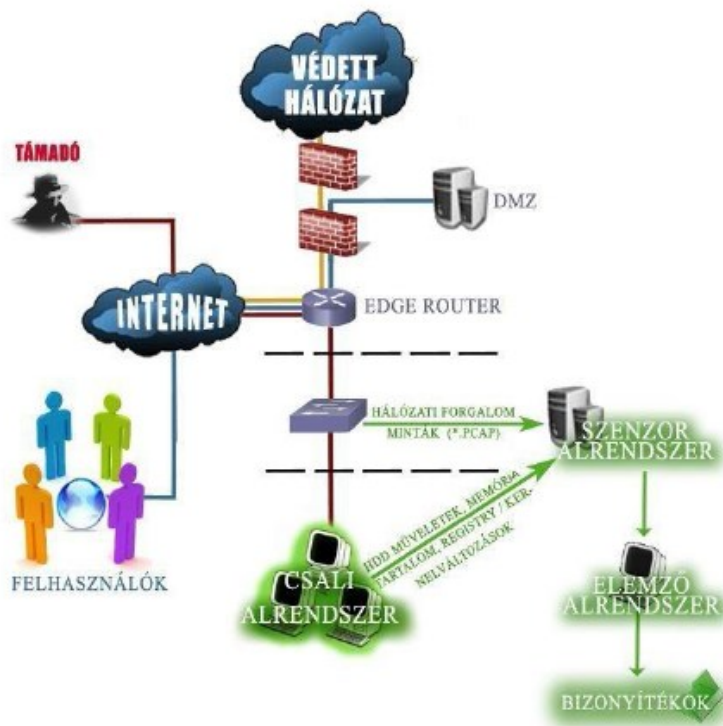
„Az Enhanced Mitigation Experience Toolkit (EMET) eszközkészlet a szoftveres biztonsági rések kihasználása elleni védekezésben nyújt segítséget, amihez a biztonsági kockázatok mértékének csökkentésére alkalmas technológiákat vesz igénybe. Ezek a technológiák olyan speciális védelmet és akadályokat jelentenek, melyeket a szoftveres biztonsági réseket kihasználni szándékozó támadóknak külön le kell győzniük. Az alkalmazott kockázatcsökkentő technológiák nem garantálják, hogy a biztonsági rések nem használhatók ki, de a lehető legnehezebbé teszik az ilyen irányú tevékenységeket.” – Microsoft Support

Az EMET nem csak az operációs rendszer, hanem bármilyen szoftver védelmére is használható. Nem csak a Microsoft szoftvereihez alkalmazható, hanem más gyártók termékeihez is, azonban bizonyos szoftverek inkompatibilisek lehetnek az EMET eszközkészlettel. Telepítés után csak be kell állítani, hogy mely szoftvereket kívánjuk védeni. Lehetőség van vállalati rendszerekre történő központi telepítésre is. A beállításokat akár csoportházirendek alkalmazásával is elvégezhetjük.

Egy jellemzően használt biztonsági megoldás a fájl integritás figyelés. Egy futó folyamat figyeli és jóváhagyja az operációs rendszer és alkalmazási fájlokat, pl. könyvtárakat, konfigurációs kulcsokat és értékeket. Ez a jóváhagyás egy ellenőrzési módszer része, mely a fájlrendszer eredeti és vizsgált állapota között történik. Az összehasonlítás gyakran magában foglalja a fájlokról készült ellenőrzési összegének összehasonlítását, de más fájl attribútumok is figyelésre kerülhetnek. Ez a módszer segít kiszűrni azokat a módosításokat, melyek nem a megfelelő működés következményei és egy esetleges behatolás előfutárait jelentik.

2.2.2 Honeypot rendszerek, mint védelmi szolgáltatások

A honeypot rendszerek hálózati csatlakozók, erőforrások, operációs rendszerek és szolgáltatások emulációjával a valós támadások detektálására szolgál. Amellett, hogy detektálja a támadási szándékot, képes rögzíteni a támadási módszert, a támadó tevékenységét is. Ezek a rendszerek a valós rendszertől teljesen különállóak, esetleges



2. ábra: Egy csali rendszer felépítése

kompromittálódásuk esetén sincs veszélyben az éles rendszer. A védelmi célú csali rendszerekre jellemző, hogy a védeni kívánt hálózathoz hasonló rendszert emulálnak.

A honeypot rendszer alkalmazása önmagában nem képes támadások megakadályozására, céljuk a védelmi szolgáltatások támogatása. Segítenek a támadás megértésében, ezzel könnyítve a hatékony védelem kidolgozását. A honeypot rendszerek széleskörűen alkalmazhatóak a hálózat védelmének fokozása érdekében, ezek körül fontosnak tartom kiemelni a következőket:

- Riasztás
- Információszerzés
- Naplózás, mintagenerálás
- Preventív védelem

2.2.2.1 Riasztás

Egy csali rendszer ellen bekövetkező biztonsági incidens esetén az értesítést küldhet az rendszergazdák számára annak bekövetkezéséről.

2.2.2.2 Információszerzés

Egy rendszer biztonságát nagymértékben növeli, ha az alkalmazott védelmi szolgáltatások naprakészek. A honeypot rendszerek segítségével megismerhetőek a támadó eszközei, módszerei és céljai. Ha ezeket ismerjük, könnyebben naprakészen tarthatjuk rendszerünket, ami nagyobb biztonságot eredményez.

2.2.2.3 Naplózás, mintagenerálás

Szinte napról napra jelennek meg új rosszindulatú kódok, mely azt jelenti, hogy a technológiai változással párhuzamosan a kártevők is változnak és frissülnek. Ezek miatt a változások miatt a vírusirtók adatbázisaiba is nehezebben kerülnek be. A honeypot rendszer azonban képes rögzíteni egy-egy támadás során a használt technikát és forgatókönyvet. Ezeket felhasználva olyan minták készíthetők, melyek bekerülve a behatolás detektáló rendszerek és vírusirtók adatbázisaiba, a későbbi behatolások során azok gyorsabb detektálását teszik lehetővé.

2.2.2.4 Preventív védelem

Amíg a támadó a csali rendszerrel foglalkozik, addig sem a valós rendszert veszélyezteti. Az úgynevezett sticky honeypot jellemző kialakítása, hogy a támadó tevékenységét lassítja, így feltartóztatva azt hosszabb időre is.

3. A VÉKONY KLIENS ARCHITEKTÚRA BEMUTATÁSA

3.1 Történeti áttekintés

A hálózatba kötött személyi számítógépek növekvő fenntartási költségei, valamint az egyre összetettebb szoftverek és újabbnál újabb biztonsági fenyegetések megjelenése arra készítette a számítástechnikában dolgozó szakértőket, hogy megvizsgálják a vékony kliens technológia megvalósíthatóságát.

Már jóval a vékony kliens terminológia számítástechnikában történő megjelenése előtt léteztek szerver alapú számítógépes rendszerek. Az első ki- és bemeneti terminálok csupán egy billentyűzetből és egy katódsugárcsőves kijelzőből álltak az adatok bevitelére és azok megjelenítésére. A korai számítógépes hardverek magas árának köszönhetően a

számítási teljesítményt és memóriát meg kellett osztani a felhasználók között és minden rendszernek szerver alapúnak kellett lennie. Ez egy valóban logikus szemlélet és megoldás volt a növekvő számítási igények tükrében, ugyanis sokkal egyszerűbb és olcsóbb volt csak ki- és bemeneti eszközöket rákötni egy már meglévő rendszerre, mint új számítógépeket vásárolni, melyek lényegesen drágábbak voltak. Ez a megoldás jelentette a dumb terminálok kezdetét. A név arra utal, hogy ezek az eszközök kizárólag ki- és bemeneti perifériák, saját számítási teljesítmény nélkül.

Az összetettebb vékony kliens architektúra kialakulása az 1970-es évek végén kezdődött, az úgynevezett X Window rendszer megjelenésének köszönhetően. Ez a felület lehetővé teszi a felhasználók számára, hogy UNIX alkalmazásokat grafikus felhasználói felületen keresztül érjenek el, egy kisebb, napjainkban személyi számítógépnek nevezett egység segítségével. Annak érdekében, hogy az X terminál és a szerver közötti adatcsere problémamentesen megtörténhessen, egy speciális, X11 nevű hálózati protokoll került kifejlesztésre és bevezetésre.

A számítási folyamatokat azonban a mikroprocesszorok és az első olyan személyi számítógépek megjelenése forradalmasította, melyek már megfelelő mennyiségű tároló kapacitással és memóriával rendelkeztek ahhoz, hogy képesek legyenek alkalmazások futtatására. A számítógép felhasználók fokozatosan fordultak el a szerver alapú rendszerektől és koncentráltak arra, hogy olyan gépeket tartsanak saját irodáikban, melyek minél nagyobb számítási teljesítménnyel és minél több alkalmazással rendelkeznek. Ez a folyamat volt jellemző sok-sok éven keresztül. Ennek ellenére 1996 körül, az Oracle és a Sun Microsystems bejelentése újra a vékony kliensek felé fordította az érdeklődést. Ez nem volt más, mint a Network Computer (NC). Az NC, az X terminálhoz hasonlóan, központosított alkalmazásokhoz és adatbázisokhoz biztosított hozzáférést a szervereken. Ezt az irányzatot követte néhány év múlva a ma már általánosan használt Citrix szoftver, amely egy hasonló protokollt vezetett be, mint az X11. Ez volt az úgynevezett Independent Computing Architecture (ICA)⁴. A vékony kliens architektúra kiforrásával egyre több egységes hardver és szoftver megoldás került kifejlesztésre. Napjainkban a HP⁵, a DellWyse⁶ és az NComputing⁷ hardver és szoftver megoldásai a legismertebb és a legsebésebb körben használt rendszerek a vékony klienses megoldások területén.

⁴ Gépfüggetlen számítógép-hálózati megoldás

⁵ <http://www8.hp.com/us/en/campaigns/thin-client-solutions/index.html>

⁶ <http://www.dell.com/us/business/p/cloud-client-computing>

⁷ <http://www.ncomputing.com>

A vékony kliens architektúra a számítástechnika egyik legdinamikusabban fejlődő ágazata. Összehasonlítva egy személyi számítógépeken alapuló hálózattal, a vékony kliensek használata jelentősen költséghatékonyabb alternatíva. A központosított rendszerek elterjedése a vékony klienseket még vonzóbbá teheti a vállalatok számára.

3.2 A vékony kliens architektúra alapjai

A vékony kliens egy olyan számítógép, amely nem rendelkezik önállóan a munkavégzéshez szükséges programok kiszolgálásához szükséges erőforrásokkal. Limitált mennyiségű memória illetve kis számítási teljesítményű processzor jellemzi. Ezeket az erőforrásokat a kliens az őt kiszolgáló szerveren, vagy akár szervereken éri el. A hagyományos személyi számítógépre épülő hálózati környezetben az alkalmazások helyben futnak és az adatok feldolgozása is a PC-n történik. A vékonykliens feladata azonban többnyire kimerül a szerver által küldött adatok megjelenítésében illetve a felhasználó által bevitt adatok és parancsok átvitelében. A kliensen nem tárolódik semmilyen fájl sem. Az adatok kezelését, feldolgozását nem maga a kliens végzi, hanem a kiszolgáló.



3. ábra: Enjay Impression Mini 1500 vékony kliens

A vékony kliensek hardveresen, fizikailag és szoftveresen is tekinthetők vékony kliensnek. A gyári vékony kliensek jellemzően nélkülöznek minden mozgó alkatrészt, így nincs bennük CD-, vagy DVD-meghajtó, merevlemez, hűtőventilátor. Csupán a néhány csatlakozó, melyekkel különböző be- és kimeneti eszközök (billentyűzet, egér, monitor) köthetők rá, illetve amelyen keresztül a hálózatra csatlakoztatható. Napjainkban már

elmaradhatatlan kelléke a vékony klienseknek is az USB csatlakozási lehetőség is. A hardveres vékony kliens mellett lehetőség van régebbi PC-ből úgynevezett szoftveres vékonykliens kialakítására is. Ehhez többféle minimális hardverigényű operációs rendszer áll rendelkezésre. A vékony kliensek használatával lehetőség nyílik desktop virtualizációs környezet könnyebb alkalmazhatóságára is, ily módon újra felhasználva egy-egy kiöregedett PC-t.

Mára már jellemzővé váltak az úgynevezett zéró kliens megoldások is. Ennek lényege, hogy a korábban meglévő erőforrásokra sincs már szükség lokálisan. Nincs operációs rendszer, vagy bármiféle tároló kapacitás. Ebben az esetben már minden számítást a szerver végez, beleértve a beviteli eszközök inputjait és a grafikus megjelenítéshez szükséges számításokat is. Ezek az eszközök csupán a közvetítő szerepét játsszák a felhasználó és a kiszolgáló között.

3.3 A vékony kliensek működése

A vékonykliensek méretükben is jelentősen különböznek a hagyományos asztali számítógépektől, azoknak csupán töredékük. Azonban a kisebb helyi számítási teljesítmény valamint a meghajtók hiánya miatt számottevő mértékű az energiafelhasználásban tapasztalható különbség. Míg egy hagyományos személyi számítógép energiafogyasztása a 85W-tól akár 110W-ig is terjedhet, addig a vékony kliensek energiaigénye minimális. Jellemzően 6-15W közötti érték.

A monitoron megjelenő információk viszont ugyanúgy jelennek meg, mint egy asztali számítógép esetében, ugyanolyan gyorsasággal. Ez annak köszönhető, hogy támogatja a grafikus felületek megjelenítését, legyen szó a támogatott operációs rendszerek bármelyikéről. Annak fényében tehát, hogy a felhasználó képernyőjén megjelenő információk gyorsan, a megszokott formában jelennek meg, a felhasználó a számára megszokott környezetben, fennakadások nélkül végezheti feladatait. Ugyanazokat a szokásos programokat használhatja, mint az asztali számítógépek esetében, legyen szó irodai programcsomagról, vagy különböző speciális szoftvekről, csupán a vékony klienses környezetben ezek az alkalmazások nem a helyi számítógépen futnak, hanem a távolban. A szerver futtatja ezeket az alkalmazásokat és feladatokat.

3.4 A vékony kliensekkel elérhető szolgáltatások

Számos olyan munkavégzéshez szükséges szolgáltatás van, amelyek igénybevételehez nem szükségesek az asztali számítógépek nyújtotta túlzott erőforrások.

Ilyenek például a különféle böngészőkből elérhető céges szoftverek, az adatbázisok elérése. De ugyanígy elég egy vékony kliens a különböző irodai programcsomagok (szövegszerkesztő, táblázatkezelő) megfelelő használatához is. Sőt, ma már nem ritka az IP feletti hangátviteli⁸ technológiát kiszolgáló vékony kliens sem.

A napjainkban jellemző nagyfelbontású audio-video és 3D tartalmak megjelenítésére azonban a korábbi vékony kliens megoldások nem alkalmasak. Azonban megjelentek olyan eszközök, amelyek lehetővé teszik e multimédiás tartalmak akár kliens oldali feldolgozását is.

3.5 Az adatközpontok

Napjainkban három alapvető csoportba sorolhatjuk a vékony kliens architektúra felhasználása során kialakított szerver oldali rendszereket:

1. Terminál szolgáltatások: ezek tipikusan a Microsoft Windows terminálszolgáltatásához vagy Távoli asztal szolgáltatásához köthető. Minden adatfeldolgozás a szerveren történik és csak a billentyű leütések és képernyőfrissítések haladnak át a hálózaton.
2. Alkalmazásvirtualizáció vagy alkalmazás közvetítés (application streaming): leegyszerűsíti egy-egy alkalmazás eljuttatását a felhasználóhoz, olyan módon, hogy az alkalmazás a kliens eszközön kerül virtualizálásra. A rendszergazdák központilag telepíthetnek és állíthatnak be egy programot és arra a helyre „közvetíthetik”, ahol arra szükség van. A program frissítését vagy hibajavítását így csak egy helyen kell elvégezni, a felhasználókhoz már a frissített verzió kerül „közvetítésre.”
3. Virtuális asztal: mely a szerveren virtuálisan létrehozott számítógépeket jelent, virtuális operációs rendszerrel, azok összes alkalmazásával együtt. Ezek a virtuális gépek a vékony kliensekről úgy érhetőek el, mintha távoli számítógépek lennének. Természetesen itt is minden adatfeldolgozás a szerveren történik, hálózati forgalmat csak a képernyőfrissítés és a különböző felhasználói bevételek jelentenek.

3.6 A kapcsolattartáshoz használt protokollok

Ahhoz, hogy a kliensek a szerverekkel kommunikálni tudjanak, mind a szervereknek, mind a klienseknek támogatniuk kell a szükséges kommunikációs protokollokat. Néhány nem annyira népszerű protokoll mellett a két legelterjedtebb ilyen protokoll a Microsoft által biztosított RDP⁹, valamint a Citrix nyújtotta ICA¹⁰. Windows

⁸ Voice over IP – VoIP. Magyarul szokás még IP-telefonia névvel is illetni.

⁹ RDP – Remote Desktop Protocol

platformokon elterjedt e protokollok támogatása. Az RDP-t nem szükséges külön a szerver oldalra is telepíteni Windows szerver esetén, hiszen azt már tartalmazza a kiszolgáló operációs rendszere. Az ICA támogatásához és teljes értékű használatához azonban külön csomagok telepítése szükséges.

Akár Windows, akár Linux alapú szerverekkel dolgozunk, a vékony kliensekre a szükséges protokollok kliens oldali részének telepítése elkerülhetetlen.

3.7 A hálózattal szemben támasztott követelmények

Ahhoz, hogy a felhasználóknak a virtuális környezetben kialakított asztalukhoz távolról csatlakozva is olyan érzésük legyen, mintha egy személyi számítógép szolgálná ki őket, elengedhetetlen a megfelelő hálózat. Azok a felhasználók által használt alkalmazások, melyek nagyon átviteli sebességet igényelnek, jobban befolyásolhatják a felhasználó tapasztalatait, mint azok, amelyek kevesebb átviteli sebességet igényelnek. A mindennapi irodai munkavégzés során a felhasználói tapasztalatot nagyban befolyásolják az adatátviteli késésben¹¹ és átviteli sebességben bekövetkező változások. A felhasználók könnyen elégedetlenné válhatnak a hálózati feltételek romlása esetén.

A legzavaróbb jelenség ebből a szempontból a nagy adatátviteli késedelem. A felhasználói tapasztalat jobban befolyásolja az adatátviteli késés növekedése, mint az átviteli sebesség csökkenése. Pusztán a sávszélesség emelésével nem javítható a felhasználói tapasztalat. Maximum 20ms lehet az adatátviteli késleltetés egy virtuális asztali környezet esetében, hogy olyan felhasználói tapasztalatot szerezhessünk, mint ha egy személyi számítógépek előtt ülénk. Emellett ehhez még 6Mbit/sec adatátviteli sebességre is szükség van.

¹⁰ ICA – Independent Computing Architecture

¹¹ Az az idő, ami a csomag elküldése és annak címzetthez való megérkezése között eltelik.

4. A VÉKONY KLIENS ARCHITEKTÚRA ELŐNYEI ÉS HÁTRÁNYAI A SZEMÉLYI SZÁMÍTÓGÉPEKKEL SZEMBEN

4.1. Előnyei az asztali számítógépekkel szemben

Egy szervezet számára nagyszámú előnnyel járhat a vékony kliens technológia alkalmazása. Tekintsük most át ezeket az előnyöket.

4.1.1. Megnövekedett élettartam

Folyamatosabb szolgáltatás elérésre lehet számítani, ugyanis a vékony kliensek számára a mozgó alkatrészek hiánya megnövekedett élettartamot biztosít, valamint jelentősen kisebb az általános felhasználásból eredő kopás és elhasználódás mértéke is. Így a kliens oldalon gyakorlatilag megszűnik a hardverek fejlesztési igénye.

4.1.2. Egyszerűsödő, központosított rendszerfelügyelet

Jelentős előnyök szerezhetőek a rendszerfelügyelet központosításával, nem csak a kiadásokban, hanem a támogatás elért szintjében és minőségében is. Minél változatosabb a szoftver környezet, annál több előnyre lehet szert tenni. Számos szoftver biztosít különböző formában távoli hozzáférést a kliensekhez. Ez lehetőséget biztosít a támogatást nyújtó személyzet számára abban, hogy egy-egy probléma megoldása során, miközben a felhasználóval beszélnek, lássák az adott felhasználó asztali felületét és azon beavatkozhasanak. Ez azonban jelentős hálózati forgalmat generál, így ha nem egy helyi hálózaton keresztül történik a kliens elérése, akkor jelentős sebesség csökkenésre lehet számítani.

Az ellenőrzött alkalmazás hozzáférésnek és tárhely használatnak köszönhetően megnöveli a produktivitást. A felhasználó csak a munkavégzéshez szükséges programokat, alkalmazásokat tudja futtatni, a kliensen nem tud nem kívánt tartalmakat tárolni.

4.1.3. Megnövekedett rendszerbiztonság

A felhasználók a szerveren lévő adatokat és alkalmazásokat kizárólag a hálózaton keresztül, megfelelő szintű felhasználói hitelesítés után érhetik el. Azt lokálisan a kliens oldalon nem tudják tárolni, köszönhetően annak, hogy a vékony kliensben nincs erre alkalmas hardver összetevő. Így a kliens oldalon csökken a biztonsági kockázat. A szerver és a kliens közötti kapcsolatért felelős protokollok titkosítják az adatokat azok átvitele előtt. Ezzel egy esetleges, átviteli közegen át történő adatszivárgás veszélyei is csökkennek, hiszen azokat a támadó nem tudja értelmezni.

A virtuális környezetben futtatott rendszereket ugyanúgy védeni kell a külső támadásoktól, ugyanolyan veszélyeknek vannak kitéve, mint a fizikai rendszerek. Vírusvédelmi szempontból ugyanolyan védelemre van szükségük. A vékony kliens architektúra alkalmazása esetén nem feltétlenül van lehetőség kliens oldali vírusvédelmi szoftverek telepítésére. Gondoljunk csak bele, létezik olyan kliens, amiben nem is található merevlemez. A megfelelő vírusvédelmet a szerveren kell kialakítani. Speciális szoftverek állnak rendelkezésre ahhoz, hogy a megfelelő védelem a kliensekre, a virtuális környezetre is kiterjeszthető legyen. Ez nem csak a felhasználói élményt fokozza, hiszen a vírusvédelmi szoftver nem foglal el memóriaterületet a kliens oldalon, hanem a vírus fertőzés kockázatát is csökkenti. A központosított vírusvédelem miatt ugyanis nem lesz olyan végpont, amelyen elavult lenne a vírusvédelmi szoftver adatbázisa, illetve a védelem már a bekapcsolás pillanatában él, hiszen a védelmi szoftver nem a kliens indulása után indul el, hanem az már a szerveren fut.

4.1.4. Megnövekedett adatbiztonság

A szervezetnél lévő adatok biztonsága az egyik kulcskérdésnek tekinthető. Vékony kliensek alkalmazásával növelhető az adatbiztonság, hiszen az adatok csak a szerveren tárolódnak. Az adatokhoz való hozzáférés a különböző felhasználói körökhöz igazítható, mindenkinek csak a saját munkájához szükséges hozzáférés biztosításával.

A felhasználói adatok, fájlok biztonsági mentése szintén könnyebb feladat egy vékony klienses környezetben, hiszen minden adat egy helyen, a szerveren tárolódik. Így azokról a rendszergazda a saját helyén ülve készíthet biztonsági másolatot, és ugyanígy egy szempillantás alatt vissza is tudja állítani. Természetesen a biztonsági mentés automatizálására is van lehetőség, és akár külső tárolóegységekre is történhetnek ezek a mentések.

4.1.5. Jelentős költség csökkenés

A vékony kliensek alkalmazásának számos, költségekkel összefüggő előnye van az asztali számítógépekkel szemben, mind kis- és közép-, mind nagyvállalati-környezetben. Gondoljunk csak a lényegesen kisebb fogyasztással járó megtakarításokra, vagy a hálózati biztonság felügyeletével kapcsolatos csökkenő kiadásokra, ha nincs a kliensen olyan szoftver, amelyet a vírusok és egyéb kártevők megfertőzhetnének.

Kis és nagy szervezetek számára a vékony kliensek költséghatékonysága ugyanúgy hosszú távon jelentkezik.

A fő infrastrukturális változást a szerver környezet kialakítása jelenti. Ebben beletartozik a vékony kliensek beszerzése, az új, összetettebb szerver környezet kialakítása és természetesen nem elhanyagolhatóan a már meglévő szerverek és asztali számítógépek cseréjéből származó költségekkel is foglalkozni kell. A TCO-ban¹² megjelenő költségek annál alacsonyabbak, minél több kliens kerül bevezetésre. Például azoknál a vállalatoknál, ahol Microsoft Configuration Manager¹³ van használatban a számítógépekre elérhető szoftverek telepítéséhez és frissítéséhez, ott a vékony kliensek frissítése csupán néhány órát fog igénybe venni, nem pedig napokat, vagy heteket. Ez kétségtelenül tekintélyes mértékű adminisztratív megtakarítás.

Ha a megtakarítások sorába beveszünk más költségkímélő tényezőket is, mint az alacsonyabb képzési költségek, maga az üzembe helyezési folyamat, az asztali gépek árához viszonyított kliensek egységára, a vékony kliensek hosszabb élettartama és a megnövekedett produktivitás, akkor a megtakarítások még inkább életképesnek tűnnek. Egyes jelentések szerint a teljes bekerülési költsége egy vékony kliensnek felhasználóra és évre lebontva kevesebb, mint a fele egy asztali számítógép költségének, ez tartalmazza a képzési és üzembe helyezési költségeket is.

A teljes bekerülési költség számításánál azonban nem csak a közvetlen pénzügyi költségeket kell figyelembe venni. A másik nagyon fontos eleme a közvetett költségek csoportja. A közvetett költségek az immateriális javakhoz kapcsolódó költségek. Ebben tartozik például a képzés vagy különböző leállások miatti termelés kiesés. Általában három csoportról beszélhetünk lágy költségek kapcsán: hardver karbantartás, alkalmazás támogatás és felhasználói támogatás. A hardverek bekerülési költsége akár a fele is lehet egy asztali számítógépes környezettel szemben, azonban a legnagyobb megtakarítás az egyéb csökkenő fenntartási költségek miatt jelentkezik. Úgy, mint csökkenő karbantartási igények, kevesebb rendszergazdai beavatkozást igénylő probléma és a felhasználói igényeket kielégíteni képes minimális IT szakértelem.

4.2. Lehetséges hátrányai

Mint ahogyan az a korábbiakban bemutatásra került, a vékony kliensen architektúrájának számos előnye van. Természetesen, mint minden technológiának, úgy

¹² Total Cost of Ownership – teljes bekerülési költség. Az IT számára a teljes bekerülési költség magában foglalja a hardver és szoftver beszerzését, kezelésének és felügyeletének költségeit, kommunikációs és végfelhasználói kiadásokat és a lehetséges leállásokhoz és egyéb termelés-kieséshez, valamint képzésekhez kapcsolódó költségeket.

¹³ Szoftver- és frissítés-terjesztési, konfigurációkezelési, hardver-szoftverleltárat megvalósító eszközök (korábbi neve Systems Management Server)

ennek is vannak korlátai, melyeket mindenképpen figyelembe kell venni egy esetleges alkalmazás előtt. Különösen igaz ez speciális igényű munkakörnyezet esetében.

4.2.1. Hálózati függőség

Mivel a vékony kliens architektúra alkalmazása esetén minden adatfeldolgozás a szerveren történik, ezért a kliensek és a szerver(ek) közötti állandó kapcsolat kulcsfontosságú. Ha a hálózati kapcsolat bármilyen hiba folytán megszűnik, a felhasználók nem tudják tovább folytatni a munkájukat, amíg a hibát el nem hárítják, a kapcsolatot helyre nem állítják. Ezzel szemben egy hagyományos szerver alapú hálózat esetén csak a különböző hálózati erőforrások, mint például megosztott fájlok vagy nyomtatók, válnak elérhetetlenné egy esetleges hálózati hiba bekövetkezésekor. Az ilyen rendszerek esetében a munkavégzés a végpontokon tovább folytatódhat a helyben futtatott alkalmazások miatt.

Nyilvánvaló tehát, hogy vékony kliensek alkalmazásakor a munkavégzés hatékonysága számottevően függ a különböző hálózati eszközök és a kiszolgáló rendszerek megbízhatóságától, a kiszolgáló rendelkezésre állásától. Ezért nagyon fontos a hálózat és a szerverek megfelelő beállítása. A szerverek esetében ezek a beállítások magukba foglalhatják a különböző feladat átvételi mechanizmusokat, a terhelés elosztást és számítógépfürtök alkalmazását.

- Feladat átvételi mechanizmusok: olyan lehetőségek, melyek azt biztosítják, hogy az eredeti rendszer összetevő meghibásodása esetén egy másik eszköz, vagy akár szoftver, automatikusan, leállás nélkül vegye át annak feladatait.
- Terhelés elosztás: az elvégzendő számítások megosztása két vagy több számítógép között. Terhelés elosztás létrehozható hardverek és szoftverek között, vagy a kettő együttes alkalmazásával. A módszer célja az optimális eszközkizhasználás, a teljesítmény növelése és az esetleges túlterhelés elkerülése.
- Számítógépfürtök alkalmazása: több számítógép összekapcsolása egy meghatározott feladat végrehajtása érdekében. Ezek a számítógépek egy egységet alkotnak, kívülről a fürtben lévők nem látszanak. Egy gép meghibásodása esetén a többi tag átveszi annak a szerepét, így biztosítva azt, hogy az ahhoz rendelt szolgáltatás továbbra is elérhető maradjon.

Mint minden hálózaton, így egy vékony kliensekkel, mint végpontokkal rendelkező hálózaton is fontos tényező az elérhető sávszélesség nagysága. Ez nagymértékben függ a hálózaton lévő felhasználók számától. A vékony kliens architektúra kialakítása miatt minden feldolgozást a szerver végez, ezért lényegesen nagyobb hálózati forgalom

generálódik. Hiszen minden feldolgozási parancsnak és eredménynek a hálózaton kell végighaladnia. Éppen ezért azoknál a felhasználói programoknál, ahol folyamatos a képernyő frissítése, mint például a CAD alkalmazások, vagy terepmodellezés, a hálózati adatforgalom elfogadhatatlanul magas szintre emelkedik. A hasonlóan magas hálózati erőforrást igénylő felhasználók esetében megoldást jelenthet a hagyományos asztali számítógépek alkalmazása.

4.2.2. Felhasználói elégedettség

Komoly problémát jelenthet az új rendszerrel szembeni ellenállás a felhasználók részéről. A CD meghajtó, a valós idejű videó és hang lejátszás képességének hiánya ugyan növelheti a termelékenységet, de valószínűleg a felhasználói elégedettséget is csökkenti. Néhány felhasználó annyira ragaszkodhat a korábban megszokott asztali környezetéhez és az ott használt programokhoz, hogy nem tudja elképzelni nélkülük a munkavégzést. A döntéshozóknak fel kell készülniük rá, hogy foglalkozni kell ezzel a problémával a vékony kliensek bevezetése előtt és után is.

4.2.3. Örökölt alkalmazások

A terminál szolgáltatások igénybe vételével több felhasználó fogja a szerveren ugyanazt az alkalmazást elérni és egyszerre használni azt. A megfelelő tanúsítvánnyal rendelkező programok az ebből eredő esetleges problémákat kellőképpen tudják majd kezelni. A speciálisan a szervezet számára készített, és az asztali környezetből örökölt programok esetében azonban fenn áll a veszélye annak, hogy a felhasználói beavatkozások felülírják a rendszerbeállításokat. Ezek a nehézségek azonban általában megoldhatóak, azonban elengedhetetlen a megfelelő tesztelés és a program esetleges újratervezése.

A vékony kliens architektúra fent említett előnyei és hátrányai azok a szempontok, melyeket mindenképpen figyelembe kell venni az áttérésre történő tervezés és a döntéshozatal időszakában. A valóság azonban azt mutatja, hogy e technológia tényleges bevezetése számos előre nem látható, meglepő eredményt hozhat. Ezek az eredmények nagyban függenek az alkalmazási környezettől is.

5. A KÜLÖNBÖZŐ ZÁRT ÉS NYÍLT FORRÁSKÓDÚ OPERÁCIÓS RENDSZEREKKEL ELLÁTOTT KLIENSEK KATONAI CÉLÚ ALKALMAZHATÓSÁGÁNAK VIZSGÁLATA

A dolgozatom első fejezetében tárgyalt, a számítógépes rendszerben kliens oldalon megjelenő hiányosságok egyik lehetséges megoldása lehet a vékony kliens architektúra alkalmazása. Véleményem szerint ezen belül is két lehetőség kínálkozik a megoldásra. Az egyik esetben a meglévő asztali számítógépek helyett új vékony kliensek beszerzésére kerülhet sor, a másik esetben pedig a már meglévő asztali számítógépeket készíthetik fel szoftveresen arra, hogy azok vékony kliensként tudjanak tovább funkcionálni. Mindkét megvalósításhoz számos megoldás áll rendelkezésre, ezeket fogom megvizsgálni, és értékelni. A végső cél egy olyan vékony kliensekből álló számítógépes környezet létrehozása lenne, amely a felhasználókat egy központosított asztali és alkalmazási környezettel látja el. Az architektúra bevezetése egységesíteni tudná a felhasználói tapasztalatot, a rendszerfelügyeletet, megnövelné a rendszer biztonságát, valamint a vezetés és irányítás hatékonyságát.

5.1 Vékony kliens eszközök

A kezdeti nehézségeiket leküzdve a vékony kliensek jelentős változáson mentek keresztül az elmúlt évtizedben. Egy központosított virtuális környezet bevezetése esetén a megfelelő vékony kliens kiválasztása döntő jelentőségű. A termékkínálat nagy, így több gyártó termékei közül is választhatunk, azonban fontos, hogy minden rendszer egyedi. És ehhez az egyediséghez igazodóan kell megválasztani a klienseket is. Meg kell határozni, hogy milyen felügyeleti megoldást kívánunk alkalmazni, hogyan tervezzük a kliensek rendszerbe iktatását, és hogy milyen más egyéb szolgáltatásokat kívánunk használni. A megfelelő vékony kliens kiválasztásához a következő szempontokat szükséges figyelembe venni:

- Központi felügyelet, mely lehetővé teszi fő irányelvek létrehozását, és azok teljesítését a vékony kliensek irányába.
- Egyszerű rendszerbe állítás, mely biztosítja az esetlegesen meghibásodó kliensek gyors cseréjét.
- Támogatott megjelenítési protokollok, hogy ne csak egyetlen szoftvergyártó termékéhez legyünk kötve, ne a gombhoz keressük a kabátot.

Egy olyan termékből, amiből rengeteg van a piacon, érdemes a piacvezető gyártók termékei közül választani, ezek ugyanis támogatni fogják az elterjedt virtualizációs technológiákat is.

5.1.1 Hewlett-Packard t620 Flexible Thin Client

Ez az eszköz a HP egyik vezető terméke, olyan impozáns megoldásokat kínál, mint az egyszerre négy kijelző megjelenítése és a PCIe x16 bővítő hely. Operációs rendszer tekintetében a Windows 7 beágyazott verzióját futtatja, de rendelhető a HP által fejlesztett Linux alapú ThinPro operációs rendszerrel is. Alapértelmezetten két magos AMD processzorral szerelik, de kérhetjük a négy magos processzorral készített változatot is, melyhez már erősebb grafikus chip is társul. Alap esetben 4GB RAM-mal szállítják, de ez egészen 16GB-ig bővíthető. Egy 10/100/1000 Ethernet szabványú csatlakozó, 6db USB port található rajta, ezek közül kettő UDB 3.0 szabványú.



4. ábra: HP t620

Írányára a hivatalos magyarországi HP webshopban¹⁴ 147 690,- Ft, melyben benne van 3 év garancia is.

5.1.2 Wyse Z90D7 (Dell)

A Wyse Z Class termékcsaládja igen népszerű a vásárlók körében. A legújabb verziója, mely a Windows 8 beágyazott verziójára épül, még nem lett a virtualizációban élen haladó gyártók által hitelesítve, így a Windows 7 alapú kliens megvizsgálását tartom ésszerűnek.

Ez a kliens egy négy magos AMD processzort használ. A Z Class termékcsalád egyik nagy előnye, hogy lehetőséget biztosít a memória széles skálán történő



5. ábra: Wyse Z90D7

bővíthetőségére, ez a D7 modell esetében egészen 32GB-ot jelent. Támogatja ezen felül az SSD meghajtókat is, és a beépített grafikus chipje FullHD (1920x1080 pixel) felbontású megjelenítésre alkalmas. Szintén rendelkezik egy 10/100/1000 Ethernet szabványú csatlakozóval, valamint 6db USB csatlakozóval, melyek közül kettő USB 3.0 szabványú. Rendelhetőek soros, párhuzamos és PS/2 port támogatással is. Ez különösen akkor lehet fontos, ha a rendszerben lévő perifériákat továbbra is használni akarjuk.

¹⁴ <http://www.hpshop.hu/?sku=F5A54AA> letöltve: 2014. 04. 06.

Irányára a Dell hivatalos webshopjában¹⁵ 679 amerikai dollár (kb. 150 000,- Ft), és ehhez is három év garanciát ad a gyártó, melyhez további terméktámogatást lehet még vásárolni.

5.1.3 IGEL UD3-430 LX

Két fajta operációs rendszerrel kerül forgalomba, az egyik egy Linux alapú, saját fejlesztésű rendszer, a másik pedig a Windows 7 beágyazott verziója. Ezek rendre 1 és 2GB memóriát tartalmaznak. Több monitoros megjelenítést is támogató grafikus chipet, 4 db USB (kettő ezek közül UDB 3.0 szabványú), egy 10/100/1000 Ethernet valamint egy PS/2 szabványú csatlakozót tartalmaz.

Legnagyobb előnye, hogy a gyárilag megvásárolt 2 év garanciát a vásárlás után, egy egyszerű termékregisztrációval 5 évre bővíthetjük, és ezért a gyártó plusz pénzt nem számol fel.



6. ábra: Igel UD3-431 LX

5.1.4 10Zig 6818v

Ez az eszköz egy AMD két magos processzort használ, 2GB memóriával, mely opcionálisan 4GB-ra bővíthető. A Windows 8 operációs rendszer beágyazott verzióját futtatja. Támogatja négy képernyő megjelenítését is, 6 USB porttal rendelkezik, ezek közül kettő USB 3.0 szabványú, valamint tartalmaz egy PCI bővítő helyet. Opcionálisan soros és párhuzamos portokkal bővíthető.

Három éves garanciát biztosít hozzá a gyártó, valamint lehetőség van kibővített cseregaranciára is.



7. ábra: 10Zig 6818v

Ezek a vékony kliens eszközök olyan nagyvállalatoknál állnak már rendszerben, mint a Boeing, vagy a Lockheed Martin. Mindegyik gyártó a saját felügyeleti termékét kínálja a vékony klienseihez, így a kialakítandó felügyelet kérdése akár eldöntheti a vékony kliensek beszerzésének vitáját is. A bemutatott eszközök a jelenleg rendszerben lévő asztali számítógépek egy jelentős részénél jobb teljesítménnyel rendelkeznek, amely számomra azt a tanulságot jelenti, hogy éppen ideje lenne lecserélni a meglévő eszközparkot.

5.2 **Meglévő asztali számítógépek újra felhasználásának lehetőségei**

A virtuális asztali infrastruktúra kialakítása nagy kiadást jelent, de a költségek egy részének egyik lehetséges minimalizálása a meglévő asztali számítógépek újra

¹⁵ <http://configure.us.dell.com/dellstore/config.aspx> letöltve: 2014. 04. 06.

felhasználása. A rendelkezésre álló személyi számítógépeket vékony kliensként is lehet alkalmazni. Ez azonban nem csak abból áll, hogy a felhasználó asztalára kirakunk egy parancsikont, mely elindítja a távoli hozzáférést a virtuális géphez. Akkor kell komolyan fontolóra venni ezt a lehetőséget, ha a kliensként használt számítógépet hajlandóak vagyunk a felhasználó előtt lezárni. Azaz, hogy a felhasználó a számítógépen helyileg futó operációs rendszerhez ne is férhessen hozzá. Fontos szempont még megvizsgálni azt is, hogy hány darab számítógépet kell ilyen módon „átalakítanunk”.

Két csoportra oszthatóak azok az eszközök, melyek segítségével az asztali számítógépekből vékony klienseket alakíthatunk ki. Az egyik csoport a Windows alapon működő átalakító eszközök, a másik pedig a vékony kliensekhez fejlesztett operációs rendszereket alkalmazó termékek.

A Windows alapú eszközök közül a ThinLaunch, Thin Desktop nevű termékek lényegében egy asztali alkalmazás, mely a helyi operációs rendszeren kerül telepítésre. Számos asztali, és beágyazott változatú Windows operációs rendszert támogat. Nem csinál mást, mint elindít egy általunk választott futtatható állományt. Ez természetesen lehet az a program, amellyel a távoli virtuális asztalhoz csatlakozunk. Így megakadályozza a felhasználót abban, hogy bármiféle helyi változtatást tudjon alkalmazni a számítógépen, vagy azon helyi alkalmazásokat futtasson. Ha virtuális környezetünkben csak alkalmazás kijánlás található, akkor azt egy webes felületre téve, és a Thin Desktop-ban a böngészőt beállítva futtatni kívánt alkalmazásnak, egyből a kijánlott alkalmazások webes felületéhez juthatunk.

A másik csoportba tartozó termékek közös vonása, hogy vagy az asztali számítógépen már meglévő Windows operációs rendszer mellé, de azt elnyomva, vagy annak helyére települnek.

- A Devon IT VDI Blaster elnevezésű vékony kliens operációs rendszer megoldása képes a meglévő operációs rendszer mellé települni, de alapértelmezetten ahhoz ezek után már nem férhet hozzá a felhasználó.
- A Wyse PC Extender egy Linux alapú vékony kliens operációs rendszer.
- A ThinStation egy ingyenes, nyílt forráskódú megoldás. Támogatja a jelentős virtualizációs platformokat, többek között a XenDesktop-ot és a Remote Desktop-ot is. Lehetőség van a számítógépre történő telepítésére is, de futtatható USB-ről LiveCD ként, vagy akár hálózatról is.

Meg kell még említeni a Linux Terminal Server Project-et is, melynek lényege, hogy a vékony kliensek a LAN hálózaton keresztül érnek el egy Linux Terminal Server-t, ami RDP protokollon keresztül a virtuális asztalok képét szolgáltatja számukra. Természetesen ezek a virtualizált asztalok akár Windows operációs rendszerek is lehetnek.

Mivel a régi asztali számítógépek újra felhasználásának sarkalatos pontja a már rajta lévő operációs rendszer, így a személyi számítógépek vékony klienssé minősítését csak átmeneti megoldásnak tartom. Azokat az eszközöket, melyek megtartják az eredeti operációs rendszert is, teljesen téves elképzelésnek tartom, hiszen csak egy plusz számítógépet jelentenek, amire a rendszergazdának időt és energiát kell fordítaniuk. Azok a megoldások azonban, melyek teljes mértékben kiváltják a meglévő operációs rendszert, megfelelő áthidaló megoldások lehetnek, amíg a számítógéppark teljes cseréje meg nem történik.

5.3 A meglévő hálózat vizsgálata a vékony kliens architektúra szükségleteinek szempontjából

A vékony kliens technológia egyik sarkalatos pontja a szerverközpontúság. Minden művelet, minden számítás a szerveren hajtodik végre. Mivel a felhasználó a hálózaton keresztül kapcsolódik a szerverhez, a szerveren futó munkamenethez, létfontosságú a hálózat olyan mértékű kiépítettsége, mely a vékony kliens technológia számára is megfelelő szintű hozzáférést és sávszélességet biztosít.

A Magyar Honvédségben a központi szolgáltatásokat nyújtó szervereken, legnagyobb arányban, a Microsoft Server operációs rendszerei futnak. A már meglévő hardveres és szoftveres eszközpark felhasználásával szerver oldalon kialakítható megoldások közül a Virtuális Desktop Infrastruktúra (VDI) és a Távoli asztal szolgáltatás (RDS¹⁶) igényelnek komolyabb szerver és hálózati erőforrásokat. A VDI alkalmazása esetén a Microsoft asztali operációs rendszerei virtuális számítógépeken futnak hardveres virtualizációs környezetben. Az RDS során a felhasználók a Server operációs rendszert érik el, mely megosztásra került a felhasználók között. Mindkét esetben lehetőség van csatlakozni mind asztali számítógépekről, mind pedig vékony kliensekről. Ezeknek a virtualizációs technológiáknak az alkalmazásával megfelelő védetségű végfelhasználói pontok alakíthatóak ki, melyek a rendszerfelügyeletet is megkönnyítik, és kellő rugalmasságot biztosítanak akkor is, ha új gépeket kell bekötni a hálózatba.

¹⁶ Remote Desktop Services

A felhasználók nagy része a központi szolgáltatásokat jelenleg is a WAN¹⁷ hálózaton keresztül éri el. A WAN hálózaton megjelenő sávszélességi és késedelmi korlátok jelentősen befolyásolhatják a Virtuális Desktop Infrastruktúra megoldás összességében vett hatékonyságát. A nagyvállalati környezetben alkalmazott virtuális asztali megoldások kihívásai magukban foglalják a VDI WAN hálózati gyenge teljesítményét, mely befolyásolhatja a felhasználók produktivitását, valamint a magas sávszélesség foglalást.

A Microsoft és a Cisco közös mérései szerint, minden egyes virtuális asztal 1Mbit/sec sávszélességet képes lefoglalni, illetve ettől jelentősen többet multimédiás alkalmazások futtatása esetén. Számos virtuális asztal alkalmazása esetén akkora forgalom generálódik, mely képes a WAN hálózat kapacitásának kimerítésére, ezáltal meghatározó mértékben rontani a felhasználói tapasztalatot. Egy virtuális asztal WAN hálózaton történő elérése jelentős adatátviteli késedelmet is jelenthet, mely lassú válaszidőkben és a monitor képének frissítési késedelmében jelenik meg. Ez szintén jelentősen rontja a felhasználói élményt.

Ahhoz, hogy teljes képet kaphassunk arról, hogy a jelenlegi hálózati kapacitás képes lenne-e kiszolgálni egy teljes mértékben központosított, és nagymértékben virtuális alapokra fektetett informatikai rendszert, meg kell vizsgálni az állandó telepítésű hálózat jelenlegi képességeit. Ehhez Bleier Attila doktori disszertációjának mérési eredményei jó alapot szolgáltatnak. Ezek az eredmények azt mutatják, hogy a legalább 1Mbit/sec, vagy annál nagyobb átviteli sebességet igénylő adatfolyamok elfogadhatatlan mértékben leterhelik a hálózatot. Ha ezt az eredményt összevetjük, a Cisco tanulmányában szereplő értékekkel, akkor nyilvánvalóvá válik, hogy egy olyan hálózaton, ahol az 1Mbit/sec átviteli sebesség súlyos leterheltséget okoz, nem megvalósíthatóak a központosított virtuális asztali eléréseket biztosító megoldások.

A Microsoft eszköztárában azonban van még egy eszköz, mely megoldást jelenthet a problémára. Ez nem más, mint a RemoteApp. Ez szolgáltatás lehetővé teszi a szerveren lévő alkalmazások távoli elérését. A felhasználó számára úgy néz ki, mintha a program a saját számítógépén futna, azonban az a szerveren fut. A felhasználók többféle módon is hozzáférhetnek ezekhez a programokhoz. Lehetőség van webes felületen keresztül történő hozzáférésre is. Mivel itt nem az egész virtuális asztalhoz fér hozzá a felhasználó, hanem csak egyes alkalmazásokhoz, így a lefoglalt sávszélesség is lényegesen kisebb lehet.

¹⁷ Wide Area Network – nagy kiterjedésű hálózat

Azonban a teljesítménymérések azt mutatják, hogy a RemoteApp és a teljes Távoli asztal hozzáférés sávszélesség felhasználása közötti különbség csekély, és az is a Távoli asztal hozzáférés javára van. Azaz, egy alkalmazás távoli elérése RemoteApp segítségével legalább ugyanakkora terhelést ró a hálózatra, mint egy teljes virtuális asztal elérése.

Úgy gondolom, hogy kizárólag Microsoft termékek használatával a jelenlegi körülmények ismeretében nem megvalósítható a komplett asztali számítógéppark vékony kliensekre történő lecserélése. Harmadik fél által készített, virtualizációs technológiákat támogató szoftverek nélkül is megoldást jelenthet erre a problémára a meglévő hálózati infrastruktúra fejlesztése.

5.4 Élet a Microsofton túl

Nem szabad azonban elhamarkodott következtetéseket levonni anélkül, hogy a többi jelentős részesedéssel rendelkező piaci szereplő termékeit is megvizsgáljunk. Számos virtuális asztal infrastruktúrát kínáló cég létezik, de a két legjelentősebb gyártó a Citrix és a VMware megoldásai a legelterjedtebbek.

5.4.1 Citrix XenDesktop

A Citrix XenDesktop egy minden részletre kiterjedő virtuális asztalt kínáló megoldás, mely a meglévő Windows asztalokhoz és alkalmazásokhoz biztosít hozzáférést, többféle kliens eszközről is. A XenDesktop segítségével lehetőség van bármilyen Windows alapú, vagy webes alkalmazás felhasználóhoz történő eljuttatására, de akár teljes virtuális asztalok kiszolgálására is lehetőséget biztosít. A kliensek fajtája igen sokrétű, a hagyományos asztali számítógépektől, a vékony klienseken át egészen az okostelefonokig terjed.

Ugyanúgy, ahogyan a Microsoft termékeinek használata esetén, más gyártók által kínált megoldások kulcskérdése szintén a hálózat, ez kapja a legfontosabb szerepet, különös tekintettel a nagy kiterjedésű hálózatok esetében. A XenDesktop esetében is fennáll, hogy az adatátviteli késés növekedésével és a sávszélesség csökkenésével jelentősen csökken a virtualizált asztalok alkalmazhatósága és a felhasználói élmény. A Citrix előállt egy olyan megoldással mely, a WAN hálózatokon lévő felhasználók számára is ugyanazt a gyorsaságot nyújtja, mintha a LAN¹⁸ hálózaton lennének. Ezt több technológia együttes alkalmazásával éri el úgy, mint a TCP csomagok optimalizációjával,

¹⁸ Local Area Network – helyi kiterjedésű hálózat

tömörítéssel, forgalom analízissal, valamint a használt távoli asztali hozzáférési technológia protokolljának optimalizálásával.

A Citrix egy átfogó elemzést készített azzal a céllal, hogy segítse azokat a vállalati döntéshozókat, akik virtuális asztali környezet bevezetését tervezik. Ennek keretében kialakított egy komplex teszt környezetet, melynek egyik fő célkitűzése az volt, hogy meghatározzák a XenDesktop átlagos sávszélesség felhasználását egy távoli eléréssel rendelkező virtuális asztalhoz csatlakozva. Ahogyan az egy ilyen tesztől elvárható, számos felhasználói alkalmazással került végrehajtásra a teszt. A mérési eredmények azt mutatják, hogy a Citrix távoli asztal hozzáférési megoldása kevesebb sávszélességet igényel, mint a Microsoft hasonló megoldása. A legmagasabb igénybevétel sem haladta meg, a 0,5Mbit/sec sávszélesség foglalt, mely az optimalizáló eszközök rendszerbe iktatásával még kisebb értéket mutatott, mindössze 0,2Mbit/sec volt.

A Citrix eszköztárában is van egy, a RemoteApp-hoz hasonló megoldás, mely a XenApp névre hallgat. A XenDesktop mérsékelt hálózati erőforrás igényét szem előtt tartva fejlesztették ki. Feladatát tekintve ugyanazt csinálja, mint a Microsoft megoldása, ugyanúgy a kiajánlott alkalmazások távoli elérését teszi lehetővé. A mérések azt mutatják, hogy a Citrix távoli alkalmazás hozzáférési megoldása szintén kevesebb hálózati sávszélességet foglal, mint a Microsoft terméke. A Citrix Xenapp esetében a maximális sávszélesség foglalt 0,11Mbit/sec volt, míg a legalacsonyabb mindössze 15kbit/sec.

Véleményem szerint, ez már egy sokkal elfogadhatóbb érték, több felhasználó egyidejű hozzáférése esetén is lehetőséget biztosít az alkalmazások hozzáféréséhez anélkül, hogy a hálózatot túlzottan nagymértékben leterhelnék. Ugyanakkor a teljes virtuális asztali hozzáférést biztosító XenDesktop hálózati erőforrás igénye bizonyos esetekben elfogadhatatlan mértékű terheltséget róna a hálózatra. Ugyan a legnagyobb terheltség esetén is csak 0,5Mbit/sec volt a sávszélesség foglalt, de ez csak egy darab távoli asztal esetén. Erre a sávszélességre minden egyes virtuális asztalnak szüksége van a távoli eléréshez. Így viszont már a jelenlegi hálózati infrastruktúra keretein belül a Citrix XenDesktop megoldása sem megvalósítható.

5.4.2 VMware View

Az egyre jobban elterjedő virtualizált asztali megoldásokhoz fejlesztette ki a VMware a saját távoli hozzáférést biztosító platformját, a View-t, mely olyan fontos piaci szereplőkként veszi fel a versenyt, mint a Microsoft Távoli asztal szolgáltatása, vagy a Citrix XenDesktop. A VMware View hasonló szolgáltatásokat nyújt, mint piaci ellenfelei.

A View egy szabadalmaztatott protokollt használ az adatok felhasználók és a kiszolgáló közti küldésére és fogadására. Eredetileg a Microsoft által nyújtott Remote Desktop Protocolt használta, de kifejlesztettek egy új, nagyteljesítményű protokollt, mely a PC over IP (PCoIP) néven ismert. A PCoIP célja, hogy túllépjen az RDP alapú távoli elérés során, az összetett grafikus tartalmak megjelenítése kapcsán tapasztalt korlátokon. A PCoIP lehetővé teszi nagy felbontású grafikai tartalom, HD minőségű hang elérését a felhasználók számára, valamint lényegesen gördülékenyebbé teszi a valós idejű mozgóképek megjelenítését. Természetesen az RDP protokollt nem számúzták, az továbbra is elérhető az alacsonyabb igényű, és kisebb sávszélességet igénylő kapcsolatok esetén a kliens gép és a virtualizált asztal között.

Természetesen a PCoIP sem a bölcsék köve, de a WAN hálózatokon előforduló változó sávszélességi korlátokhoz és adatátviteli késésekhez jól alkalmazkodik. A PCoIP esetében is számos hatékonyságot növelő módszert építettek be a protokoll alapjaiba. A PCoIP egyik megoldása, hogy a RDP-től eltérően nem TCP alapú, hanem UDP protokollt használ. Ezáltal nem kerül sor a kliens és a szerver közötti kapcsolat kiépítésére, ezzel az idővel is csökken az adatátviteli késedelem. A másik technikai megoldás, amit a PCoIP használ, az a konkurens megoldásoknál jobb tömörítési arány.

A VMware, a Citrix-hez hasonlóan, készített egy teljesítmény tanulmányt, melynek célja a megfelelő virtuális környezet kiválasztásának elősegítése. Különböző Windows asztali operációs rendszerek kerültek virtualizálásra, majd tipikus irodai használatot előidéző terhelést generáltak és vizsgálták a lefoglalt sávszélesség mértékét. WAN hálózat esetén az átlagos igénybevétel megközelítette az 1Mbit/sec átviteli értéket. Ez nem meglepő, hiszen a VMware View is RDP alapokon működik, a mért értékek pedig közel vannak a Microsoft és Cisco által mért értékhez. Ez viszont megengedhetetlenül nagy terhelést ró a meglévő hálózatra.

A különböző piaci szereplők különféle, általában a saját megoldásaikat alkalmazzák a virtuális asztalok távoli elérése kapcsán, melyek sarkalatos pontja a hálózat. Egy központosított, nagymértékben virtualizált számítógépes rendszer lényege veszhet el akkor, ha a felhasználók nem érik el a szervert, vagy a munkavégzés folyamata a hálózat leterheltsége miatt még lassabb, mint a kiöregedő asztali számítógépeken. Nem szabad továbbá elfelejtenünk azt sem, hogy a meglévő fix telepítésű hálózaton már így is jelentős mértékű forgalom generálódik nap, mint nap. A hálózat jelentős fejlesztése nélkül nem

megvalósítható az egyetlen, centralizált számítási központból álló számítástechnikai rendszer kialakítása.

A nagyobb sávszélességű hozzáféréssel rendelkező felhasználók számára, ilyenek például a Budapesten kialakított gigabites hálózati végpontokhoz csatlakozó felhasználók, a központosított, egységes informatikai rendszer kialakítása megoldható lenne. Azonban a jelenlegi inhomogén rendszert tovább bonyolítani nincs értelme. Ezen fejlesztések hatékonyságát akkor lehetne kihasználni, ha az összes helyőrséget be tudjuk kapcsolni az új rendszerbe, erre azonban a jelenlegi hálózat nem ad lehetőséget.

5.5 Vékony kliens jellegű eszközök tábori alkalmazhatósága

Hiába van lehetőség a katonai szervezet hálózatára csatlakozni, ha azt csak körülményesen használható, nehéz számítógépekkel lehet megvalósítani. Terepen, tábori körülmények között használt számítástechnikai eszközök az egyik legfontosabb előnye a hordozhatóság. Egy laptop használata erre a célra már megfelelő lehet, különösen, ha azt egy járműben használják. Napjainkban már elérhetőek olyan, mindössze tenyér méretű számítógépek is, melyek katonai felhasználását érdemes megvizsgálni. Az egyik ilyen eszköz a Raspberry Pi.

5.5.1 *A Raspberry pi bemutatása*

A Raspberry Pi nem más, mint egy egyetlen áramköri lapra szerelt számítógép. Természetesen, ahogy nagyobb testvéreit, így ezt is monitorra tudjuk kötni, egérrel és billentyűzettel vezérelni. Minden olyan munkára alkalmas, amire egy hagyományos asztali számítógépet is általában használnak a felhasználók. Lehet rajta



8. ábra: Raspberry Pi

dokumentumot szerkeszteni, Internetezni, sőt, az integrált grafikus feldolgozó egységének köszönhetően még HD videó lejátszására is alkalmas. Eredetileg ugyan oktatási célból hozták létre, de mint koncepciót mindenképpen érdemes megvizsgálunk. Egy olcsó, ultrakönyű, alacsony energia felhasználású eszközről van szó. Az ehhez hasonló eszközök alkalmazása megkönnyítheti a felhasználók feladat végrehajtását tábori körülmények között.

5.5.2 *Raspberry Pi, mint vékony kliens*

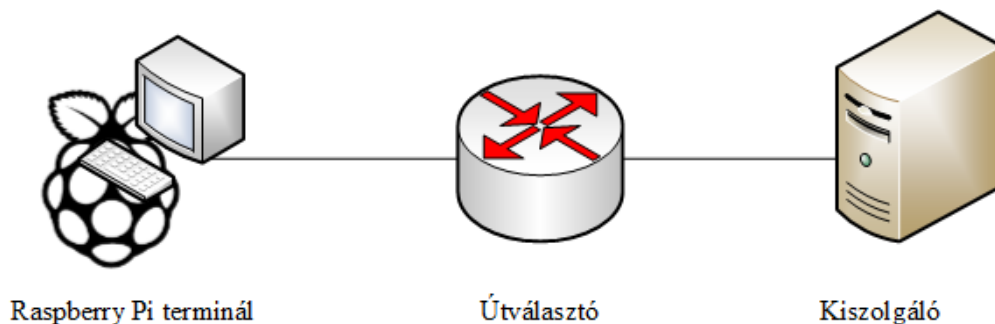
Mint minden számítógép, így a Raspberry Pi is rendelkezik operációs rendszerrel. Többféle operációs rendszert is támogat, ezek nagy része valamilyen Linux disztribúció. Ennek köszönhetően lehetőség van másik operációs rendszerek távoli elérésére is. Sőt, egy internetes project is létezik a Raspberry Pi vékony klienssé változtatására. Ennek keretében egy olyan Linux disztribúció került kialakításra, melybe beépítésre kerültek a fő piaci szereplők távoli asztali elérést biztosító lehetőségei úgy, mint a Microsoft RDP, VMWare View, Citrix Receiver, illetve ezeken kívül még számos, távoli kapcsolatot biztosító megoldás.

A Magyar Honvédségben már rendszeresített Híradó és Informatikai Központ állomásban (HIK) megtalálható szerver lehetőséget biztosítana egy tábori vékony klienst alkalmazó felhasználónak a szerverhez való távoli kapcsolódásra. Ezek után a felhasználó már a szerver erőforrásait kihasználva tudná feladatait végrehajtani.

A Raspberry Pi-t vékony kliensként történő alkalmazására számos bemutató található az Interneten. Ezek jellemzően otthoni felhasználási körülmények közötti vizsgálatok. Ezekből azonban számomra nem derült ki, hogy valójában mennyire alkalmas ez az eszköz erre a feladatra. Ennek érdekében összeállítottam egy otthoni hálózatot, egy kiszolgáló „szerverrel”, egy útválasztóval, valamint egy Raspberry Pi-vel. Céлом az volt, hogy első kézből szerezhessenek tapasztalatot a Raspberry Pi ilyen irányú képességeiről.

5.5.2.1 *A környezet kialakítása, eszközbeállítások*

A kiszolgáló gépen egy Windows 8.1 operációs rendszer fut, ehhez akartam távoli eléréssel csatlakozni. Ennek érdekében engedélyezésre került a számítógép távoli elérése, valamint létrehoztam egy általános jogkörrel rendelkező felhasználót, amellyel majd be tudok jelentkezni. A Raspberry Pi-re a Raspbian elnevezésű operációs rendszer került, mely egy Debian alapú disztribúció.



9. ábra: Raspberry Pi tesztkörnyezet

Ahhoz, hogy a távoli elérés lehetségessé váljon, az rdesktop nevű, nyílt forráskódú távoli asztali klienst telepítettem. Ehhez egy terminal ablakban a következő parancs kiadása szükséges:

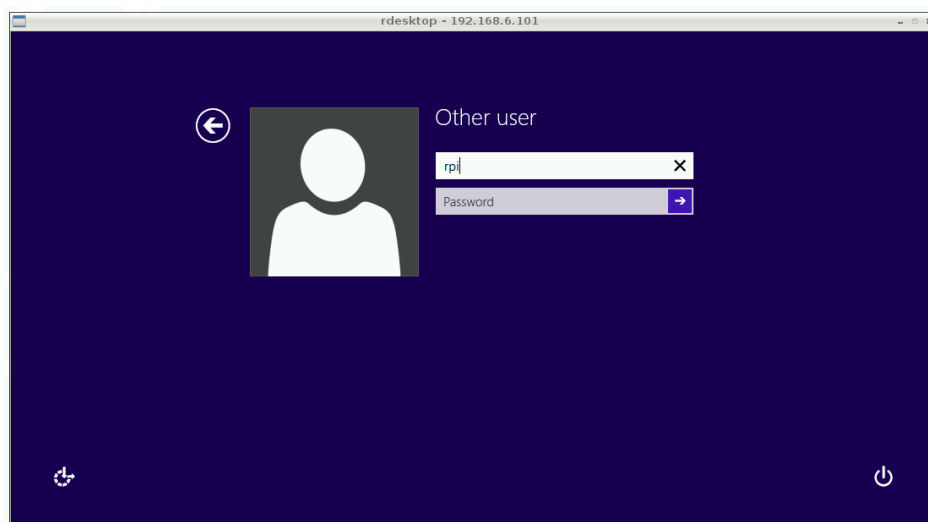
```
sudo apt-get install rdesktop
```

Ezután már nincs más hátra, mint maga a bejelentkezés. Az rdesktop súgójában részletesen le van írva a használat módja, illetve a kapcsolók listája is, melyek segítségével paraméterezhetjük a kliens programot. Létrehoztam egy bash script fájlt, mely a következőket tartalmazza:

```
rdesktop -u rpi -p - -k hu -g 60% 192.168.6.100
```

- rdesktop: az rdesktop kliens indítására vonatkozó utasítás
- -u rpi: a bejelentkezéshez használt felhasználónév
- -p -: a -p kapcsoló a jelszavas bejelentkezéshez szükséges. Nem célszerű ezt egy egyszerű, kódolatlan fájlban tárolni, ezért nem került bele a jelszó, helyette csak egy kötőjel, így a bejelentkezés során a felhasználónak meg kell adnia jelszavát.
- -k hu: a magyar billentyűzet kiosztás kényszerítése a távoli kapcsolat során
- -g 60%: a képernyő méretének beállítása. Itt lehetőség van szélesség*magasság alakban pixelpontosan is megadni azt a méretet, melyben a távoli asztal megjelenik. Jelen esetben ez a maximálisan megjeleníthető kép 60%-a.
- 192.168.6.100: a kiszolgáló IP címe.

A fájl elindítása után egyből a bejelentkezési képernyő fogad.



10. ábra: Windows bejelentkezési képernyő, távoli eléréssel

Ezután különböző felhasználói programokat futtattam és közben figyelemmel kísértem a Raspberry Pi processzor és memória használatát. Az rdesktop alkalmazás közel 3MB memóriát foglalt le induláskor, és ez a futás során nem változott. Valamint azt tapasztaltam még, hogy a távoli asztali elérés csak akkor jelentett processzorhasználatot, ha a megjelenítendő kép változott. Egy görgetés, vagy ablakváltás után, mikor már kirajzolódott a teljes kép, a processzorhasználat lecsökkent. Az eredményekből az olvasható ki, hogy azon alkalmazások és tartalmak megjelenítése jelent nagyobb igénybevételt, melyek változatos grafikus tartalommal rendelkeznek. Ilyen például egy internetes hírportál betöltése és böngészése is. Az egyszerű felületű tartalmak megjelenítése nem kifejezetten erőforrás igényes. Ilyen például egy Microsoft Word, vagy Excel dokumentum szerkesztése, de egy kevés képpel és dinamikus tartalommal nem rendelkező weboldal is. A multimédiás tartalmak megjelenítése azonban már nagyobb kihívás, rendkívül magas processzor kihasználást jelent és élvezhetetlen felhasználói élménnyel párosul. Nem csak a távoli hozzáférés alkalmazás jelent ebben az esetben nagy processzorterhelést, hanem a gazda operációs rendszer grafikus megjelenítésért felelős komponense is. A kettő együtt már maximális processzorhasználatot eredményez.

	CPU MIN	CPU MAX	CPU AVE.
Word	1%	12%	6,5%
Excel	1%	3%	2%
Internetes tartalom, sok képpel	6%	30%	18%
Internetes tartalom, főleg szöveges	3%	12%	7,5%
Multimédia	46%	50%	48%

A fenti táblázatban az rdesktop folyamatának processzor igénye látható. A sok képes tartalom nélküli megjelenítés nem jelentett problémát, egyedül a Word dokumentumban és a böngészés során előforduló néhány kép miatt emelkedett meg a processzor kihasználtsága. Ezen dokumentumok olvasása korrekt felhasználói élményt biztosít, viszont a képek és egy-egy nagyobb görgetés esetén megakad a megjelenítés, ugrik egyet a kép, ami zavaró.

Ugyanez mondható el a komplexebb, képekkel teletűzdelt weboldalak böngészéséről is. A képek megjelenítése akadozik, zavaró, különösen a napjainkban

jellemző felületű, óriási képekkel teletűzdelt hírportálok esetében. Nehézséget jelent már a főoldal átfutása is, mert a folyamatos ugrálás zavaró, megnehezíti az olvasást is.

A multimédiás tartalom egy 640*360 képkocka felbontású, 29 képkocka/másodperc képkockasebességgel rendelkező videó volt. Már ennél a ma már alacsony felbontásnál is élvezhetetlenül akadozott a kép megjelenítése. A problémát az jelentette, hogy a videó 29 képkocka/másodperc frissítési rátáját a távoli asztal protokoll nem volt képes kezelni.

A Raspberry Pi eredetileg oktatási cézzal készült, limitált erőforrásokkal. Ez a korlátozottság az általam elvégzett tesztek során is megmutatkozott. Az operációs rendszeri háttér miatt nagyon sok alacsony erőforrás igényű alkalmazást képes futtatni, mint amilyen például az rdesktop kliens. Az eszköz vékony kliensként történő alkalmazhatóságát ezen tesztek elvégzése és tapasztalatai alapján nem tartom ésszerűnek. A lehetőség adott, a technikai háttér biztosított, azonban a felhasználói tapasztalat nem hozta a várt eredményeket. Az eredeti, oktatási célzat azonban e teszt során is megmutatkozott, a Windows távoli eléréséről és a Raspberry Pi-ről is rengeteg új információt szereztem.

BEFEJEZÉS

A vékony kliensek hatásos alternatívát jelenthetnek az asztali számítógépekkel szemben. Nem csak azért lehetnek vonzóak, mert hosszú távon olcsóbbak, mint a személyi számítógépek, de üzemeltetésük, felügyeletük is egyszerűbb, mindemellett jelentősen megnövelik a hálózat biztonságát is. Ahogyan arra dolgozatomban is kitértem, a vékony kliensek energiafelhasználása jelentősen kevesebb az asztali számítógépekhez viszonyítva. A kisebb energiafogyasztás pedig kisebb villanyszámlát is jelent, így ez a megtakarítások között jelentkezik. Hosszú távon újabb komoly költségmegtakarítást jelent az is, hogy a vékony kliensek élettartama hosszabb, mint egy személyi számítógépé. Az is jelentős érv a vékony kliensek használata mellett, hogy teljes életciklusuk alatt könnyebb naprakészen tartani.

A vékony kliensek, egy megfelelő környezetben, képesek a legnagyobb mértékben elterjedt alkalmazások futtatására. Felhasználó barát környezetet biztosítanak és felhasználásuk nem bonyolultabb egy személyi számítógépénél. Az örökölt alkalmazások virtuális környezetben történő futtatása azonban jelenthet problémát. A meglévő személyi számítógépek rendszerben tartásának költségei azonban egyre inkább csak emelkedni fognak. Sajnos azonban a jelenlegi állandó telepítésű hálózat inhomogén felépítése miatt a vékony kliens architektúra Magyar Honvédségben történő bevezetése korlátokba ütközik. Azokon a végfelhasználói pontokon, ahol a hálózati követelmények teljesülnek, lehetőség lenne rá. Jellemzően ilyenek a kis távolságú, tábori LAN hálózatba kapcsolt zászlóalj, és dandár törzs munkaadások. A központi kiszolgálótól nagy távolságra elhelyezkedő hozzáférési pontokon azonban az adatátvitelben olyan komoly mértékű minőségi romlás következne be, amely már ellehetetlenítené a rendszer felhasználását. A megoldás az lehetne, ha nem egyetlen adatközpont kerülne kialakításra, hanem minden helyőrségben lokális kiszolgálókat állítanának rendszerbe, így megoldódnának az átviteltechnikai berendezések alacsony adatátviteli sebességéből, és rossz minőségéből eredő összeköttetési problémák. Azonban a jelenlegi számítógépes rendszer további bonyolítása sem anyagi, sem pedig rendszerfelügyeleti szempontból nem lenne szerencsés.

A modern hadseregek informatikai függése ma már megkérdőjelezhetetlen. Nem csak a kommunikáció és az irányítás területén, hanem a mindennapi, irodai feladatok elvégzése esetében is. A számítástechnikai eszközök fejlődése nem fog megállni és várható, hogy egyre inkább szükség lesz rá a mindennapi felhasználás területén. Így tehát kézenfekvő az olyan megoldások keresése és alkalmazása, melyek költség hatékonyabbak,

mint a hagyományos asztali számítógépek alkalmazása. Ennek az igénynek a kiszolgálására a vékony kliensek alkalmazása egy lehetséges megoldást jelent.

IRODALOMJEGYZÉK

- Net-talking toaster to burn news onto bread kész
http://www.theregister.co.uk/2008/09/11/wacky_toaster/ letöltve: 2014. 04. 17.
- Nehezen szabadulunk a sebezhető Java verzióktól
<http://biztonsagportal.hu/nehezen-szabadulunk-a-sebezhető-java-verzioktól.html>
letöltve: 2014. 03. 17.
- Kaspersky Lab Report: Java under attack – the evolution of exploits in 2012-2013
http://www.securelist.com/en/analysis/204792310/Kaspersky_Lab_Report_Java_under_attack_the_evolution_of_exploits_in_2012_2013 letöltve: 2014. 03. 17.
- Mark Burgess, *Principles of Network and System Administration, Second Edition*, John Wiley & Sons Ltd, West Sussex, 2004.
- Villano, Matt. "Is thin in? Will the 'new' thin client contain spiraling campus computing and support costs, or is it just the 21st century's dumb terminal?" *The Free Library* 2004.
http://www.thefreelibrary.com/Is_thin_in?_Will_the_'new'_thin_client_contain_spiraling_campus...-a0117681911 letöltve: 2014. 02. 14.
- Bisbal, J., Lawless, D., Wu, B. & Grimson, J., "Legacy Information Systems: Issues and Directions", *IEEE Software*, 16, pp. 103-111. (1999).
- Bodlaki Ákos, Csikely Judit, Endrédi Gábor, (szerk.: Muha Lajos), *Az informatikai biztonság kézikönyve* Verlag Dashöfer Szakkiadó, Budapest, 2007.
- A biztonsági kockázatok csökkentésére szolgáló Enhanced Mitigation Experience Toolkit eszközkészlet
<http://support.microsoft.com/kb/2458544/hu> letöltve: 2014. 03. 18.
- File Integrity Monitoring
<http://www.ionx.co.uk/products/verisys/how-it-works> letöltve: 2014. 03. 18.
- Assure system integrity: Besz of breed file integrity monitoring
<http://www.tripwire.com/it-security-software/scm/file-integrity-monitoring/>
letöltve: 2014. 03. 20.
- Szabó András, „Preventív hálózatzvédelmi rendszerek alkalmazási lehetőségei a támadások detektálására, valamint a módszerek elemzésére I. rész”, *Hadmérnök*, 6:(4) pp. 1-11. (2011)
- Martin Courtney, „Whatever happened to thin clients?” *Engineering and Technology Magazine*, 8. évf., 1. szám 2013.
- Windows Thin PC Whitepaper v1.0
<http://download.microsoft.com/download/E/E/7/EE740852-95D2-48F2-A661-0771E693E620/Windows%20Thin%20PC%20Whitepaper%20v1%200.pdf>
letöltve: 2014. 01. 19.
- Environmental Benefits of Thin Computing Whitepaper March 2009.
<http://www.wyse.com/Dell-Wyse-Environmental-Benefits-whitepaper.pdf> letöltve: 2014.02. 23.
- Total Cost of Ownership (TCO)
<http://www.gartner.com/it-glossary/total-cost-of-ownership-tco> letöltve: 2014. 02. 25.
- Virtual Security - Anti-Virus megoldások
<http://fortinet.hu/php/keret.php?m=8&hk=155> letöltve: 2014. 02. 26.
- Nasimuddin Ansari, Shekhar Tiwari, Neeraj Agrawal, *Practical Handbook of Thin-Client Implementation*, NewAge International (P) Ltd., Publishers, New Delhi, 2008.

- Total Cost of Ownership Comparison of PCs With Server-Based Computing
<http://web.citrix.com/go/m2l/hi/pdf/GartnerReport.pdf> letöltve: 2014. 03. 30.
- Becta - British Educational Communications and Technology Agency - Technical papers, Thin client networking
http://webarchive.nationalarchives.gov.uk/20101102103654/foi.becta.org.uk/content_files/corporate/resources/technology_and_education_research/thin_client.pdf
letöltve: 2014. 02. 12.
- Virtual Desktop Performance and Quality of Experience
<http://www.tmcnet.com/redir/?u=1006143> letöltve: 2014. 04. 20.
- Newburn Consulting, Thin Client Benefits (White Paper), 2002. Barrie David
http://www.thinclient.net/pdf/Thin_Client_Benefits_Paper.pdf letöltve: 2014. 03. 26.
- HA (High Availability) cluster építése
[http://unixlinux.tmit.bme.hu/HA_\(High_Availability\)_cluster_építése](http://unixlinux.tmit.bme.hu/HA_(High_Availability)_cluster_építése) letöltve: 2014. 02. 14.
- Use what you already own to lower the TCO of your desktop virtualization project, 2011
http://www.thinlaunch.com/pdf/Use_what_you_already_own_for_Desktop_Virtualization.pdf letöltve: 2014. 04. 04.
- More tools for converting PCs to thin clients
<http://searchvirtualdesktop.techtarget.com/tip/More-tools-for-converting-PCs-to-thin-clients> letöltve: 2014. 04. 04.
- HP FLEXIBLE CLIENTS
<http://www8.hp.com/us/en/campaigns/thin-client-solutions/t620.html> letöltve: 2014. 04. 06.
- High-performance Virtual Desktop | Wyse Z class Thin Client
<http://www.dell.com/us/business/p/wyse-z-class/pd> letöltve: 2014. 04. 06.
- IGEL IZ3/UD3 Series
<https://www.igel.com/products/thin-client-zero-client-hardware/iz3ud3-series.html>
letöltve: 2014. 04. 06.
- 6818v Thin Client
<http://www.10zig.com/product/thin-clients-for-vdi/185/> letöltve: 2014. 04. 16.
- Cisco Wide Area Application Services and Microsoft RDP 7.1: Optimize VDI Delivery over the WAN, 2010.
http://www.cisco.com/c/dam/en/us/products/collateral/routers/2800-series-integrated-services-routers-isr/white_paper_c11-683601.pdf letöltve: 2014. 03. 25.
- Bleier Attila, *A Magyar Honvédség állandó telepítésű hálózatának modernizációja*, Zrínyi Miklós Nemzetvédelmi Egyetem, Bolyai János Katonai Műszaki Kar, Katonai Műszaki Doktori Iskola, Budapest, 2010.
- Performance Assessment and Bandwidth Analysis for Delivering XenDesktop to Branch Offices, 2010.
http://support.citrix.com/servlet/KbServlet/download/23001-102-673657/XenDesktop%20to%20Branch%20Offices_v2.pdf letöltve: 2014. 03. 26.
- VMware Horizon View 5.2 Performance and Best Practices, 2013.
<https://www.vmware.com/files/pdf/view/vmware-horizon-view-best-practices-performance-study.pdf> letöltve: 2014. 03. 26.
- Raspberry Pi
<http://www.raspberrypi.org/> letöltve: 2014. 04. 20.

- Raspberry Pi Thin Client
<http://rpitc.blogspot.com/> letöltve: 2014. 04. 20.
- Híradó és Informatikai Központ (HIK) állomás Beépítési és rendszertechnikai terve, 2007.

ÁBRAJEGYZÉK

1. ábra: IBM személyi számítógép	11
Forrás: http://www-03.ibm.com/ibm/history/exhibits/pc/images/overlay/02101.jpg letöltve: 2014. 04. 20.	
2. ábra: Egy csali rendszer felépítése	13
Forrás: Szabó András, „Preventív hálózatvédelmi rendszerek alkalmazási lehetőségei a támadások detektálására, valamint a módszerek elemzésére I. rész”, <i>Hadmérnök</i> , 6:(4) pp. 1-11. (2011)	
3. ábra: Enjay Impression Mini 1500 vékony kliens	16
Forrás: http://galaxycomputer.net/images/Thin-Client.jpg letöltve: 2014. 04. 20.	
4. ábra: HP t620	26
Forrás: http://www.www8-hp.com/us/en/images/hero_t620_tcm_245_1534847.jpg letöltve: 2014. 04. 20.	
5. ábra: Wyse Z90D7	26
Forrás: http://www.square1.nl/wp-content/uploads/2013/10/Zw-angle-left-400_9.png letöltve: 2014. 04. 20.	
6. ábra: Igel UD3-431 LX	27
Forrás: http://www.instant-axess.co.uk/prod_images_blowup/UD34.jpg letöltve: 2014. 04. 20.	
7. ábra: 10Zig 6818v	27
Forrás: http://www.thinclientstore.com/image/cache/data/10ZiG/6817v/10zig%206817v-500x500.png letöltve: 2014. 04. 20.	
8. ábra: Raspberry Pi	34
Forrás: http://malnapc.hu/wp-content/gallery/malna-pc-kepek/Raspberry_Pi-B-01_75_2.jpg letöltve: 2014. 04. 20.	
9. ábra: Raspberry Pi tesztkörnyezet	35
Forrás: saját	
10. ábra: Windows bejelentkezési képernyő, távoli eléréssel	36
Forrás: saját	